*Red Hat Network 3.7*

# Reference Guide

**Red Hat Network 3.7: Reference Guide**
Copyright © 2005 by Red Hat, Inc.

Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

RHNref(EN)-3.7-RHI (2005-03-16T12:14)
Copyright © 2005 by Red Hat, Inc. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, V1.0 or later (the latest version is presently available at http://www.opencontent.org/openpub/).
Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.
Distribution of the work or derivative of the work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.
Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.
All other trademarks referenced herein are the property of their respective owners.
The GPG fingerprint of the security@redhat.com key is:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

# Table of Contents

**Introduction to the Guide** ..... **i**
1. Document Conventions ..... i
2. More to Come ..... iv
2.1. Send in Your Feedback ..... iv
**1. Red Hat Network Overview** ..... **1**
1.1. Demo ..... 2
1.2. Update ..... 2
1.3. Management ..... 2
1.4. Provisioning ..... 3
1.5. Monitoring ..... 4
1.6. Errata Notifications and Scheduled Package Installations ..... 4
1.7. Security, Quality Assurance, and Red Hat Network ..... 4
1.8. Before You Begin ..... 5
**2. Red Hat Update Agent** ..... **7**
2.1. Starting the **Red Hat Update Agent** ..... 7
2.2. Registration ..... 9
2.2.1. Registering a User Account ..... 11
2.2.2. Registering a System Profile ..... 14
2.3. Setup and Use ..... 18
2.3.1. Choosing a Software Channel ..... 19
2.3.2. Choosing Packages to Update ..... 19
2.3.3. Installing Updated Packages ..... 24
2.3.4. Update Agent Finished ..... 25
2.3.5. Command Line Version ..... 26
2.4. Configuration ..... 30
2.4.1. Using the **Red Hat Update Agent Configuration Tool** ..... 30
2.4.2. Command Line Version ..... 33
2.5. Registering with Activation Keys ..... 34
**3. Red Hat Network Daemon** ..... **37**
3.1. Configuring ..... 37
3.2. Viewing Status ..... 37
3.3. Disabling ..... 37
3.4. Troubleshooting ..... 37
**4. Red Hat Network Alert Notification Tool** ..... **39**
4.1. Configuring the Applet ..... 39
4.2. Notification Icons ..... 40
4.3. Viewing Updates ..... 41
4.4. Applying Updates ..... 41
4.5. Launching the RHN Website ..... 41
**5. Red Hat Network Registration Client** ..... **43**
5.1. Configuring the **Red Hat Network Registration Client** ..... 43
5.2. Starting the **Red Hat Network Registration Client** ..... 44
5.3. Registering a User Account ..... 47
5.4. Registering a System Profile ..... 49
5.4.1. Hardware System Profile ..... 49
5.4.2. Software System Profile ..... 50
5.5. Finishing Registration ..... 52
5.6. Entitling Your System ..... 54
5.7. Text Mode RHN Registration Client ..... 54

**6. Red Hat Network Website ..... 57**
6.1. Navigation ..... 57
6.1.1. Entitlement Views ..... 57
6.1.2. Categories and Pages ..... 57
6.1.3. Errata Alert Icons ..... 59
6.1.4. Quick Search ..... 59
6.1.5. Systems Selected ..... 59
6.1.6. Lists ..... 59
6.2. Logging into the RHN Website ..... 60
6.3. Your RHN ..... 60
6.3.1. Your Account ..... 62
6.3.2. Your Preferences ..... 63
6.3.3. Purchase History ..... 63
6.3.4. Help ..... 63
6.4. Systems ..... 64
6.4.1. Overview — ..... 65
6.4.2. Systems ..... 66
6.4.3. System Groups — ..... 76
6.4.4. System Set Manager — ..... 79
6.4.5. System Entitlements ..... 84
6.4.6. Advanced Search — ..... 85
6.4.7. Activation Keys — ..... 85
6.4.8. Stored Profiles — ..... 87
6.4.9. Custom System Info — ..... 87
6.4.10. Kickstart — ..... 87
6.5. Errata ..... 94
6.5.1. Relevant Errata ..... 95
6.5.2. All Errata ..... 95
6.5.3. Advanced Search ..... 97
6.6. Channels ..... 97
6.6.1. Software Channels ..... 97
6.6.2. Channel Entitlements ..... 101
6.6.3. Easy ISOs ..... 101
6.6.4. Package Search ..... 101
6.6.5. Software Packages ..... 101
6.6.6. Manage Config Channels — ..... 103
6.7. Schedule ..... 109
6.7.1. Pending Actions ..... 109
6.7.2. Failed Actions ..... 110
6.7.3. Completed Actions ..... 110
6.7.4. Archived Actions ..... 110
6.7.5. Actions List ..... 110
6.8. Users — ..... 111
6.8.1. User Roles ..... 112
6.8.2. User List — ..... 112
6.9. Monitoring — ..... 115
6.9.1. Probe Status — ..... 115
6.9.2. Notification — ..... 118
6.9.3. Scout Config Push — ..... 118
6.9.4. General Config — ..... 118

**7. Monitoring** ..... **119**
7.1. Prerequisites ..... 119
7.2. Red Hat Network Monitoring Daemon (`rhnmd`) ..... 119
7.2.1. Probes requiring the daemon ..... 120
7.2.2. Installing the Red Hat Network Monitoring Daemon ..... 120
7.2.3. Configuring SSH ..... 121
7.2.4. Installing the SSH key ..... 121
7.3. Notifications ..... 122
7.3.1. Creating Notification Methods ..... 122
7.3.2. Receiving Notifications ..... 123
7.3.3. Redirecting Notifications ..... 123
7.3.4. Filtering Notifications ..... 124
7.3.5. Deleting Notification Methods ..... 124
7.4. Probes ..... 124
7.4.1. Managing Probes ..... 125
7.4.2. Establishing Thresholds ..... 125
7.4.3. Monitoring the RHN Server ..... 126
7.5. Troubleshooting ..... 126
7.5.1. Examining Probes with `rhn-catalog` ..... 126
7.5.2. Viewing the output of `rhn-runprobe` ..... 127
**A. Command Line Config Management Tools** ..... **129**
A.1. **Red Hat Network Configuration Client** ..... 129
A.1.1. Listing Config Files ..... 129
A.1.2. Getting a Config File ..... 129
A.1.3. Viewing Config Channels ..... 129
A.1.4. Differentiating between Config Files ..... 130
A.1.5. Verifying Config Files ..... 130
A.2. **Red Hat Network Configuration Manager** ..... 130
A.2.1. Creating a Config Channel ..... 131
A.2.2. Adding Files to a Config Channel ..... 131
A.2.3. Differentiating between Latest Config Files ..... 132
A.2.4. Differentiating between Various Versions ..... 132
A.2.5. Downloading All Files in a Channel ..... 133
A.2.6. Getting the Contents of a File ..... 133
A.2.7. Listing All Files in a Channel ..... 133
A.2.8. Listing All Config Channels ..... 134
A.2.9. Removing a File from a Channel ..... 134
A.2.10. Deleting a Config Channel ..... 134
A.2.11. Determining the Number of File Revisions ..... 134
A.2.12. Updating a File in a Channel ..... 135
A.2.13. Uploading Multiple Files at Once ..... 135
**B. RHN API Access** ..... **137**
B.1. Using the auth Class and Getting the Session ..... 137
B.2. Obtaining the system_id ..... 137
B.3. Determining the sid ..... 137
B.4. Viewing the cid ..... 137
B.5. Getting the sgid ..... 138
B.6. Sample API Script ..... 138

**C. Probes ..... 141**
C.1. Probe guidelines ..... 141
C.2. Apache 1.3.x and 2.0.x ..... 141
C.2.1. Apache::Processes ..... 142
C.2.2. Apache::Traffic ..... 142
C.2.3. Apache::Uptime ..... 143
C.3. BEA WebLogic 6.x and higher ..... 143
C.3.1. BEA WebLogic::Execute Queue ..... 144
C.3.2. BEA WebLogic::Heap Free ..... 144
C.3.3. BEA WebLogic::JDBC Connection Pool ..... 145
C.3.4. BEA WebLogic::Server State ..... 146
C.3.5. BEA WebLogic::Servlet ..... 146
C.4. General ..... 147
C.4.1. General::Remote Program ..... 147
C.4.2. General::Remote Program with Data ..... 147
C.4.3. General::SNMP Check ..... 148
C.4.4. General::TCP Check ..... 149
C.4.5. General::UDP Check ..... 149
C.4.6. General::Uptime (SNMP) ..... 150
C.5. Linux ..... 150
C.5.1. Linux::CPU Usage ..... 150
C.5.2. Linux::Disk IO Throughput ..... 151
C.5.3. Linux::Disk Usage ..... 151
C.5.4. Linux::Inodes ..... 152
C.5.5. Linux::Interface Traffic ..... 152
C.5.6. Linux::Load ..... 153
C.5.7. Linux::Memory Usage ..... 153
C.5.8. Linux::Process Counts by State ..... 154
C.5.9. Linux::Process Count Total ..... 154
C.5.10. Linux::Process Health ..... 155
C.5.11. Linux::Process Running ..... 156
C.5.12. Linux::Swap Usage ..... 156
C.5.13. Linux::TCP Connections by State ..... 157
C.5.14. Linux::Users ..... 158
C.5.15. Linux::Virtual Memory ..... 158
C.6. LogAgent ..... 159
C.6.1. LogAgent::Log Pattern Match ..... 159
C.6.2. LogAgent::Log Size ..... 160
C.7. MySQL 3.23 - 3.33 ..... 161
C.7.1. MySQL::Database Accessibility ..... 161
C.7.2. MySQL::Opened Tables ..... 161
C.7.3. MySQL::Open Tables ..... 161
C.7.4. MySQL::Query Rate ..... 162
C.7.5. MySQL::Threads Running ..... 162
C.8. Network Services ..... 163
C.8.1. Network Services::DNS Lookup ..... 163
C.8.2. Network Services::FTP ..... 163
C.8.3. Network Services::IMAP Mail ..... 164
C.8.4. Network Services::Mail Transfer (SMTP) ..... 164
C.8.5. Network Services::Ping ..... 165
C.8.6. Network Services::POP Mail ..... 165
C.8.7. Network Services::Remote Ping ..... 166
C.8.8. Network Services::RPCService ..... 167
C.8.9. Network Services::Secure Web Server (HTTPS) ..... 167
C.8.10. Network Services::SSH ..... 168
C.8.11. Network Services::Web Server (HTTP) ..... 168

C.9. Oracle 8i and 9i ..... 169
C.9.1. Oracle::Active Sessions ..... 169
C.9.2. Oracle::Availability ..... 170
C.9.3. Oracle::Blocking Sessions ..... 170
C.9.4. Oracle::Buffer Cache ..... 171
C.9.5. Oracle::Client Connectivity ..... 171
C.9.6. Oracle::Data Dictionary Cache ..... 172
C.9.7. Oracle::Disk Sort Ratio ..... 172
C.9.8. Oracle::Idle Sessions ..... 173
C.9.9. Oracle::Index Extents ..... 173
C.9.10. Oracle::Library Cache ..... 174
C.9.11. Oracle::Locks ..... 175
C.9.12. Oracle::Redo Log ..... 175
C.9.13. Oracle::Table Extents ..... 176
C.9.14. Oracle::Tablespace Usage ..... 176
C.9.15. Oracle::TNS Ping ..... 177
C.10. RHN Satellite Server ..... 177
C.10.1. RHN Satellite Server::Disk Space ..... 177
C.10.2. RHN Satellite Server::Execution Time ..... 178
C.10.3. RHN Satellite Server::Interface Traffic ..... 178
C.10.4. RHN Satellite Server::Latency ..... 179
C.10.5. RHN Satellite Server::Load ..... 179
C.10.6. RHN Satellite Server::Probe Count ..... 179
C.10.7. RHN Satellite Server::Process Counts ..... 180
C.10.8. RHN Satellite Server::Processes ..... 180
C.10.9. RHN Satellite Server::Process Health ..... 181
C.10.10. RHN Satellite Server::Process Running ..... 182
C.10.11. RHN Satellite Server::Swap ..... 182
C.10.12. RHN Satellite Server::Users ..... 182
**Glossary ..... 183**
**Index ..... 189**

# Introduction to the Guide

Welcome to the *Red Hat Network 3.7 Reference Guide*. The *RHN Reference Guide* will guide you through registering your system with Red Hat Network and using its many features.

Since Red Hat Network offers a variety of service levels, from the most basic Update module to the most advanced Monitoring package, some content of this guide may be inapplicable to you. This is particularly true of the RHN website, which displays selected categories, pages, and tabs depending on the entitlement level of the account used to log in. Refer to Chapter 6 *Red Hat Network Website* to determine what is available to you.

Depending on which version of Red Hat Enterprise Linux you have installed, the **Red Hat Network Registration Client** and the **Red Hat Update Agent** might be different than the ones described in this manual as new features are added. Once you use Red Hat Network to update these applications, you can use the latest version of this manual.

All versions of this manual are available in HTML and PDF formats at http://www.redhat.com/docs/manuals/RHNetwork/.

This version of the manual covers version 4.2.38 of the Red Hat Enterprise Linux 3 **Red Hat Update Agent** and versions 2.9.14 and 2.9.12 of the Red Hat Enterprise Linux 2.1 **Red Hat Update Agent** and **Red Hat Network Registration Client**, respectively.

**Warning**

Systems running Red Hat Enterprise Linux 2.1 will need to use the separate **Red Hat Network Registration Client** before starting the **Red Hat Update Agent**. Refer to Chapter 5 ***Red Hat Network Registration Client*** for instructions. Systems running Red Hat Enterprise Linux 3 can go directly to the **Red Hat Update Agent**, which has registration functionality built in. Refer to Chapter 2 ***Red Hat Update Agent*** for instructions.

For an overview of Red Hat Network offerings, please review the descriptions available at http://www.redhat.com/software/rhn/ .

## 1. Document Conventions

When you read this manual, certain words are represented in different fonts, typefaces, sizes, and weights. This highlighting is systematic; different words are represented in the same style to indicate their inclusion in a specific category. The types of words that are represented this way include the following:

`command`

Linux commands (and other operating system commands, when used) are represented this way. This style should indicate to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Sometimes a command contains words that would be displayed in a different style on their own (such as file names). In these cases, they are considered to be part of the command, so the entire phrase is displayed as a command. For example:

Use the `cat testfile` command to view the contents of a file, named `testfile`, in the current working directory.

`file name`

File names, directory names, paths, and RPM package names are represented this way. This style should indicate that a particular file or directory exists by that name on your system. Examples:

The `.bashrc` file in your home directory contains bash shell definitions and aliases for your own use.

The `/etc/fstab` file contains information about different system devices and file systems.

Install the `webalizer` RPM if you want to use a Web server log file analysis program.

**application**

This style indicates that the program is an end-user application (as opposed to system software). For example:

Use **Mozilla** to browse the Web.

[key]

A key on the keyboard is shown in this style. For example:

To use [Tab] completion, type in a character and then press the [Tab] key. Your terminal displays the list of files in the directory that start with that letter.

[key]-[combination]

A combination of keystrokes is represented in this way. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

**text found on a GUI interface**

A title, word, or phrase found on a GUI interface screen or window is shown in this style. Text shown in this style is being used to identify a particular GUI screen or an element on a GUI screen (such as text associated with a checkbox or field). Example:

Select the **Require Password** checkbox if you would like your screensaver to require a password before stopping.

**top level of a menu on a GUI screen or window**

A word in this style indicates that the word is the top level of a pulldown menu. If you click on the word on the GUI screen, the rest of the menu should appear. For example:

Under **File** on a GNOME terminal, the **New Tab** option allows you to open multiple shell prompts in the same window.

If you need to type in a sequence of commands from a GUI menu, they are shown like the following example:

Go to **Applications** (the main menu on the panel) => **Programming** => **Emacs Text Editor** to start the **Emacs** text editor.

**button on a GUI screen or window**

This style indicates that the text can be found on a clickable button on a GUI screen. For example:

Click on the **Back** button to return to the webpage you last viewed.

`computer output`

Text in this style indicates text displayed to a shell prompt such as error messages and responses to commands. For example:

The `ls` command displays the contents of a directory. For example:

```
Desktop          about.html      logs          paulwesterberg.png
Mail             backupfiles     mail          reports
```

The output returned in response to the command (in this case, the contents of the directory) is shown in this style.

`prompt`

A prompt, which is a computer's way of signifying that it is ready for you to input something, is shown in this style. Examples:

```
$
#
[stephen@maturin stephen]$
leopard login:
```

**`user input`**

Text that the user has to type, either on the command line, or into a text box on a GUI screen, is displayed in this style. In the following example, **`text`** is displayed in this style:

To boot your system into the text based installation program, you must type in the **`text`** command at the `boot:` prompt.

*`<replaceable>`*

Text used for examples, which is meant to be replaced with data provided by the user, is displayed in this style. In the following example, *`<version-number>`* is displayed in this style:

The directory for the kernel source is `/usr/src/kernels/`*`<version-number>`*`/`, where *`<version-number>`* is the version and type of kernel installed on this system.

Additionally, we use several different strategies to draw your attention to certain pieces of information. In order of how critical the information is to your system, these items are marked as a note, tip, important, caution, or warning. For example:

**Note**

Remember that Linux is case sensitive. In other words, a rose is not a ROSE is not a rOsE.

**Tip**

The directory `/usr/share/doc/` contains additional documentation for packages installed on your system.

**Important**

If you modify the DHCP configuration file, the changes do not take effect until you restart the DHCP daemon.

**Caution**

Do not perform routine tasks as root — use a regular user account unless you need to use the root account for system administration tasks.

**Warning**

Be careful to remove only the necessary partitions. Removing other partitions could result in data loss or a corrupted system environment.

## 2. More to Come

The *Red Hat Network Reference Guide* is constantly expanding as new Red Hat Network features and service plans are launched. HTML and PDF versions of this and other manuals are available within the **Help** section of the RHN website and at http://www.redhat.com/docs/.

**Note**

Although this manual reflects the most current information possible, read the *RHN Release Notes* for information that may not have been available prior to our documentation being finalized. The notes can be found on the RHN website and at http://www.redhat.com/docs/.

### 2.1. Send in Your Feedback

If you would like to make suggestions about the *Red Hat Network Reference Guide*, please submit a report in Bugzilla: http://bugzilla.redhat.com/bugzilla/

Be sure to select the Red Hat Network product and the Documentation component. To easily associate the problem with this guide, mention its identifier:

RHNref(EN)-3.7-RHI (2005-03-16T12:14)

redhat

# Chapter 1.

# Red Hat Network Overview

Have you ever read about a new version of a software package and wanted to install it but could not find it?

Have you ever tried to find an RPM through an Internet search engine or an RPM repository and been linked to a site that you have never heard of?

Have you ever tried to find an RPM but instead found only the source files that you had to compile yourself?

Have you ever spent hours or even days visiting different websites to see if you have the latest packages installed on your system, only to have to do it again in a few months?

Those days are over with Red Hat Network (RHN). RHN provides the solution to all your system software management needs.

Red Hat Network is an Internet solution for managing a Red Hat Enterprise Linux system or a network of Red Hat Enterprise Linux systems. All Security Alerts, Bug Fix Alerts, and Enhancement Alerts (collectively known as Errata Alerts) can be downloaded directly from Red Hat or your own custom collection. You can even have updates scheduled to be delivered directly to your system as soon as they are released.

The main components of Red Hat Network are as follows:

- the **Red Hat Update Agent**
- the Red Hat Network website, whether this is hosted by the central RHN Servers, an RHN Satellite Server or fed through an RHN Proxy Server
- Red Hat Network Daemon
- the **Red Hat Network Registration Client** - for systems running Red Hat Enterprise Linux 2.1 only.

The **Red Hat Update Agent** (`up2date`) provides your initial connection to Red Hat Network. Once registered, it enables channel subscription, package installs, and management of System Profiles. Red Hat Enterprise Linux 3 and newer systems will even use the Red Hat Update Agent to register with RHN. See Chapter 2 ***Red Hat Update Agent*** for further information.

Although both the RHN website and the **Red Hat Update Agent** allow you to view Errata Alerts from the Red Hat Errata list and apply updates, the website offers a much more granular view of your account and provides added functionality required for management and provisioning of systems. For enterprise deployments of Red Hat Network, the website is a must.

The **Red Hat Network Daemon** (`rhnsd`) runs in the background as a service and probes the Red Hat Network for notifications and updates at set time intervals (see Chapter 3 *Red Hat Network Daemon* for further information). This daemon is necessary if you want to schedule updates or other actions through the website.

The **Red Hat Network Registration Client** allows you to register your Red Hat Enterprise Linux 2.1 systems with RHN. (Newer versions of Red Hat Enterprise Linux have registration functionality built into the **Red Hat Update Agent**.) Registration involves creating a unique RHN username and password, probing the hardware on your system to create a Hardware Profile, and probing the software packages installed on your system to create a Package Profile. This information is sent to RHN, and RHN returns a unique System ID to your system. See Chapter 5 ***Red Hat Network Registration Client*** for more information.

Many Red Hat Network terms are used throughout this manual. As you read the *Red Hat Network Reference Guide*, refer to the *Glossary* as necessary for an explanation of common terms.

**Tip**

For a comparison chart of RHN service levels, refer to http://www.redhat.com/software/rhn/table/.

## 1.1. Demo

The RHN Demo service level is the complimentary service level. All users receive one free subscription to RHN Demo. All that is required is the completion of a brief survey once every 60 days.

With each Demo subscription, you receive:

- Errata Notifications — Be the first to know about Red Hat's patches. Subscribe to email errata notification through Red Hat Network.
- Errata Updates — Immediately bring individual systems up-to-date with the click of a button.
- Search Packages — Search through the full repository of RPMs available to Red Hat Network users.
- Search Errata — Search through the collection of all errata ever released through Red Hat Network.

## 1.2. Update

The RHN Update service is ideal for a user with one Red Hat Enterprise Linux system or a small number of Red Hat Enterprise Linux systems to keep updated. Subscription to Update can be purchased at http://rhn.redhat.com/purchase_info.pxt.

With each Update subscription, you receive the essential functionality provided to Demo users, plus:

- Easy ISOs — For customers who have purchased subscriptions to Red Hat Network, ISO images are available for immediate download.
- Priority Access during periods of high load — When Red Hat releases a large errata, users with Priority Access can be guaranteed that they will be able to access the updated packages immediately.
- RHN Support Access — All paying customers of Red Hat Network receive web based support for their RHN questions.
- Errata Notification, Multiple Systems — Subscriptions for multiple systems means Errata notification for Errata to all of those systems. Note that only one email is distributed per each Errata, regardless of the number of systems affected.
- Errata Updates, Multiple Systems — Get quick updates for multiple systems with an easy button click for each system.

## 1.3. Management

In addition to the features offered in the RHN Demo and Update subscription levels, the RHN Management subscription service allows you to manage your network of Red Hat Enterprise Linux systems, users, and system groups through its **System Set Manager** interface.

RHN Management is based upon the concept of an organization. Each Management-level Red Hat customer has the ability to establish users who have administration privileges to system groups. An

Organization Administrator has overall control over each Red Hat Network organization with the ability to add and remove systems and users. When users other than the Organization Administrator log into the Red Hat Network website, they see only the systems they have permission to administer.

To create an account that can be used to entitle systems to RHN Management, go to https://rhn.redhat.com/ and click on the **Create Account** link under the **Sign In** fields. On the *Sign Up for Red Hat Network* page, click **Create a new Corporate Login**. After creating a corporate account, you may add users within your organization to it.

The Red Hat Network features available to you depend on the subscription level for each Red Hat Enterprise Linux system. With each Management subscription, you receive the functionality provided to Demo and Update users, plus:

- Package Profile Comparison — Compare the package set on a system with the package sets of similar systems with one click.
- Search Systems — Search through systems based on a number of criteria: packages, networking information, even hardware asset tags.
- System Grouping — Web servers, database servers, workstations and other workload-focused systems may be grouped so that each set can be administered in common ways.
- Multiple Administrators — Administrators may be given rights to particular system groups, easing the burden of system management over very large organizations.
- System Set Manager — You may now apply actions to sets of systems instead of single systems. Work with members of a predefined system group, or work with an ad-hoc collection of systems. Install a single software package to each, subscribe the systems to a new channel, or apply all Errata to them with a single action.
- Batch Processing — Figuring out a list of outdated packages for a thousand systems would take days for a dedicated sysadmin. Red Hat Network Management service can do it for you in seconds.

## 1.4. Provisioning

As the highest management service level, RHN Provisioning encompasses all of the features offered in the RHN Demo, Update, and Management subscription levels. It is designed to allow you to deploy and manage your network of Red Hat Enterprise Linux systems, users, and system groups.

Like, Management, Provisioning is based upon an organization. But it takes this concept a step further by enabling customers with Provisioning entitlements to kickstart, reconfigure, track, and revert systems on the fly.

In addition to all of the features mentioned in lower service levels, Provisioning provides:

- Kickstarting — Systems with Provisioning entitlements may be re-installed through RHN with a whole host of options established in kickstart profiles. Options include everything from the type of bootloader and time zone to packages included/excluded and IP address ranges allowed. Even GPG and SSL keys can be pre-configured.
- Client Configuration — Customers may use RHN to manage the configuration files on Provisioning-entitled systems. Users can upload files to RHN's central configuration manager, verify local configuration files against those stored by RHN, and deploy files from RHN. Further, custom configuration channels can be created to help manage this process.
- Snapshot Rollbacks — Provisioning-level users have the ability to revert the package profile, configuration files, and RHN settings of systems. This is possible because snapshots are captured whenever an action takes place on a system. These snapshots identify groups, channels, packages, and configuration files.

- Custom System Information — Provisioning customers may identify any type of information they choose about their systems. This differs from the more rigorous System Profile information and the completely arbitrary Notes in that it allows you to develop specific keys of your choosing and then assign searchable values for that key to each Provisioning-entitled system. For instance, this feature would allow you to identify the cubicle in which each system is located.

## 1.5. Monitoring

Unlike the other service levels, RHN Monitoring does not include the systems management functions of other entitlements. Instead it is a separate entitlement available to Management- and Provisioning-level customers with Red Hat Enterprise Linux systems.

Monitoring allows an organization to install probes that can immediately detect failures and identify performance degradation before it becomes critical. Used properly, the Monitoring entitlement can give you insight into the applications, services, and devices on each system.

Specifically, Monitoring provides:

- Probes — Dozens of probes can be run against each system. These range from simple `ping` checks to custom remote programs designed to return valuable data.
- Notification — Alerts resulting from probes entering WARNING and CRITICAL states can be sent to email and pager addresses with contact methods identified by you. Each probe notification can be sent to a different method, or address.
- Central Status — The results of all probes are summarized in a single **Probe Status** page, with the systems affected broken down by state.
- Reporting — By selecting a probe and identifying the particular metric and a range of time, you can generate graphs and event logs depicting precisely how the probe has performed.

## 1.6. Errata Notifications and Scheduled Package Installations

You can configure Red Hat Network to send you email notifications of new and updated software packages as soon as the packages are available through RHN. You receive one email per Errata, regardless of the number of your systems affected. You can also schedule package installs or package updates. The benefits include:

- Reduced time and effort required by system administrators to stay on top of the Red Hat Errata list
- Minimized security vulnerabilities in your network by providing the patches as soon as Red Hat releases them
- Filtered list of package updates (packages not relevant to your network are not included)
- Reliable method of managing multiple systems with similar configurations

## 1.7. Security, Quality Assurance, and Red Hat Network

Red Hat Network provides significant benefits to your network including security and quality assurance. All transactions made between you and Red Hat Network are encrypted, and all RPM packages are signed with Red Hat's GNU Privacy Guard (GPG) signature to ensure authenticity.

Red Hat Network incorporates the following security measures:

1. Your System Profile available at http://rhn.redhat.com is accessible only with an RHN-verified username and password.

2. A Digital Certificate is written to the client system after registration and is used to authenticate the system during each transaction between the client and Red Hat Network. The file is only readable by the root user on the client system.
3. All notifications and information messages are signed by Red Hat with an electronic signature using GPG. RPM can be used to verify the authenticity of the package before it is installed.
4. All transactions are encrypted using a Secure Sockets Layer (SSL) connection.
5. All packages are tested and verified by the Red Hat Quality Assurance Team before they are added to the Red Hat Errata list and Red Hat Network.

## 1.8. Before You Begin

By default, all the software packages you need to use Red Hat Network are installed with Red Hat distributions. However, if you chose not to install them during the installation process, you will need to obtain the **Red Hat Update Agent** (`up2date`) and possibly the **Red Hat Network Registration Client** (`rhn_register`). In Red Hat Enterprise Linux 3, registration functionality is built into the **Red Hat Update Agent**, while Red Hat Enterprise Linux 2.1 users will need the **Red Hat Network Registration Client**.

**Warning**

The SSL certificate packaged with older versions of the **Red Hat Update Agent** and the **Red Hat Network Registration Client** reached its end of life August 28, 2003. Users attempting to connect using this certificate will receive SSL connection or certificate verification errors. You may view and obtain the versions of these applications containing new certificates at the RHN Client Software page. In the RHN website, click **Help** at the top-right corner, **Get RHN Software** in the left navigation bar, and scroll down to examine the packages and versions.

To determine the versions of the client applications installed, run the `rpm -q` command followed by the package name. For instance, for the **Red Hat Network Registration Client**, type the following command:

```
rpm -q rhn_register
```

If the **Red Hat Network Registration Client** is installed, it will return something similar to:

```
rhn_register-2.9.3-1
```

The version number might differ slightly.

If you do not have the **Red Hat Network Registration Client** installed, the command will return:

```
package rhn_register is not installed
```

Perform this check for every package in Table 1-1 relevant to your system. Remember, only Red Hat Enterprise Linux 2.1 users need the separate **Red Hat Network Registration Client**. If you prefer to use the command line versions, you do not have to install the two packages ending in `gnome`.

| Package Name | Description |
|---|---|
| `rhn_register` | Provides the **Red Hat Network Registration Client** program and the text mode interface |

| Package Name | Description |
|---|---|
| `rhn_register-gnome` | Provides the GNOME interface (graphical version) for the **Red Hat Network Registration Client**; runs if the X Window System is available |
| `up2date` | Provides the **Red Hat Update Agent** command line version and the Red Hat Network Daemon |
| `up2date-gnome` | Provides the GNOME interface (graphical version) for the **Red Hat Update Agent**; runs if the X Window System is available |

**Table 1-1. Red Hat Network Packages**

# Chapter 2.

# Red Hat Update Agent

The **Red Hat Update Agent** is your connection to Red Hat Network. It enables you to register your systems, create System Profiles, and alter the settings by which your organization and RHN interact. Once registered, your systems can use the **Red Hat Update Agent** to retrieve the latest software packages from Red Hat. This tool will allow you to always have the most up-to-date Red Hat Enterprise Linux systems with all security patches, bug fixes, and software package enhancements.

Remember, this tool must be run on the system you wish to update. You cannot use the **Red Hat Update Agent** on the system if it is not entitled to an RHN service offering.

**Warning**

Only systems running Red Hat Enterprise Linux 3 can use the **Red Hat Update Agent** to register with RHN. Systems running Red Hat Enterprise Linux 2.1 will need to use the separate **Red Hat Network Registration Client** before starting the **Red Hat Update Agent**. Refer to Chapter 5 ***Red Hat Network Registration Client*** for instructions. Then return to this chapter for instructions on using the **Red Hat Update Agent**.

**Important**

You must use **Red Hat Update Agent** Version 2.5.4 or higher to upgrade your kernel automatically. It will install the updated kernel and configure LILO or GRUB to boot the new kernel the next time the system is rebooted. To ensure you are running the latest version, execute the command `up2date up2date`. If you do not have the latest version installed, this command will update it.

## 2.1. Starting the Red Hat Update Agent

If you are not running the X Window System or prefer the command line version of the **Red Hat Update Agent**, skip to Section 2.3.5 *Command Line Version*.

You must be root to run the **Red Hat Update Agent**. If you start it as a standard user, you will be prompted to enter the root password before proceeding. The **Red Hat Update Agent** can be started using one of the following methods:

For Red Hat Enterprise Linux 3:

- On the GNOME and KDE desktops, go to the **Main Menu Button** (on the Panel) => **System Tools** => **Red Hat Network**.
- At a shell prompt (for example, an xterm or gnome-terminal), type the command `up2date`.

For Red Hat Enterprise Linux 2.1:

- On the GNOME desktop, go to the **Main Menu Button** (on the Panel) => **Programs** => **System** => **Update Agent**.
- On the KDE desktop, go to the **Main Menu Button** (on the Panel) => **Update Agent**.
- At a shell prompt (for example, an xterm or gnome-terminal), type the command `up2date`.

If you choose the last option and start the application from a shell prompt, you can specify the options in Table 2-1 to the **Red Hat Update Agent**. To view these options, type the command `up2date --help`.

For example, use the following command to specify the directory in which to download the updated packages (temporarily overriding your saved configuration):

```
up2date --tmpdir=/tmp/up2date
```

| Argument | Description |
|---|---|
| `--configure` | Configure **Red Hat Update Agent** options. Refer to Section 2.4 *Configuration* for detailed instructions. |
| `-d`, `--download` | Download packages only; do not install them. This argument temporarily overrides the configuration option **Do not install packages after retrieval.** Use this option if you prefer to install the packages manually. |
| `-f`, `--force` | Force package installation. This option temporarily overrides the file, package, and configuration skip lists. |
| `-i`, `--install` | Install packages after they are downloaded. This argument temporarily overrides the configuration option **Do not install packages after retrieval.** |
| `-k`, `--packagedir` | Specify a colon separated path of directories to look for packages before trying to download them. |
| `--nosig` | Do not use GPG to check package signatures. This option temporarily overrides the saved configuration option. |
| `--tmpdir=`*`directory`* | Temporarily override the configured package directory. The default location is `/var/spool/up2date`. This option is useful if you do not have enough space in the configured location. |
| `--justdb` | Only add packages to the database and do not install them. |
| `--dbpath=`*`dir`* | Specify an alternate RPM database to use temporarily. |

**Table 2-1. Graphical Update Agent Options**

The first time you run the **Red Hat Update Agent**, two dialog boxes will appear that you will not see in subsequent startups: Configure Proxy Server and Install GPG Key.

As shown in Figure 2-1, the first dialog box to appear will prompt you for HTTP Proxy Server information. This is useful if your network connection requires you to use a proxy server to make HTTP connections. To use this feature, select the **Enable HTTP Proxy** checkbox and type your proxy server in the text field with the format http://HOST:PORT, such as **`http://squid.mysite.org:3128`**. Additionally, if your proxy server requires a username and password, select the **Use Authentication** checkbox and enter your username and password in the respective text fields.

An HTTP Proxy Server is not required by Red Hat Network. If you do not want to use this feature, click the **OK** button without making any selections. Note that the Red Hat Network Server dropdown menu at the top of the dialog box is only useful to RHN Proxy and Satellite customers. These customers should refer to the RHN Client Configuration Guide for registration steps. Also note this dialox box is actually the **General** tab of the **Red Hat Update Agent Configuration Tool**. Refer to Section 2.4 *Configuration* for detailed instructions.

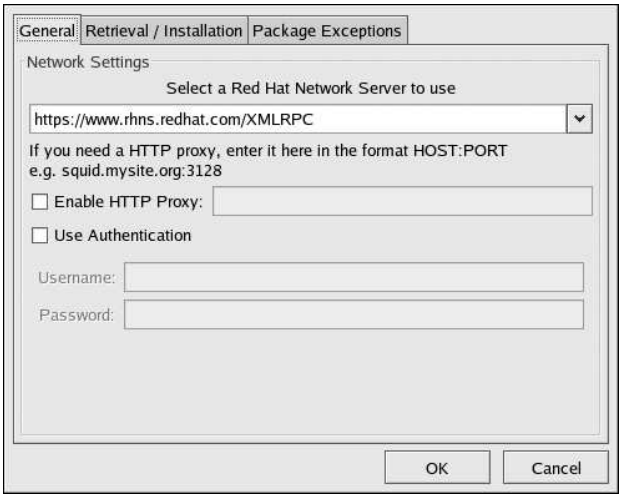


**Figure 2-1. Configure Proxy Server**

The second dialog box to appear will prompt you to install the Red Hat GPG key, as shown in Figure 2-2. This key is used to verify the packages you download for security purposes. Click **Yes** to install the key, and you will not see this message again.

Your GPG keyring does not contain the Red Hat, Inc. public key.
Without it, you will be unable to verify that packages Update Agent downloads are securely signed by Red Hat.
Your Update Agent options specify that you want to use GPG.
To install the key, run the following as root:
rpm --import /usr/share/rhn/RPM-GPG-KEY
Install key?
No
Yes

**Figure 2-2. Install GPG Key**

## 2.2. Registration

Before you begin using Red Hat Network, you need to create a username, password, and System Profile. Upon launch, the **Red Hat Update Agent** senses whether these tasks have been accomplished. If not, it guides you through the registration process. If you ever need to force the **Red Hat Update Agent** into registration mode, say to re-register an existing system, you may do so by issuing the following command at a shell prompt:

```
up2date --register
```

**Important**

If your username is part of a larger organizational account, you should take caution when registering your systems. By default, all systems registered with the **Red Hat Update Agent** end up in the Ungrouped section of systems visible only to Organization Administrators. To ensure you retain management of these systems, Red Hat recommends your organization create an activation key associated with a specific system group and grant you permissions to that group. You may then register your systems using that activation key and find those System Profiles within RHN immediately. Refer to Section 2.5 *Registering with Activation Keys* for instructions.

After installing the Red Hat GPG key, the screen in Figure 2-3 will appear. It appears every time you start the **Red Hat Update Agent**. Click **Forward** to continue.

Welcome to Red Hat Update Agent
This is Red Hat Update Agent. It will assist you in updating your Red Hat Linux system with the latest software available from Red Hat Network.
To continue, click "Forward." To cancel without updating anything, click "CANCEL."
Cancel
Back
Forward

**Figure 2-3. Welcome Screen**

After clicking through the Welcome Screen, the Red Hat Privacy Statement appears. (See Figure 2-4). Red Hat is committed to protecting your privacy. The information gathered during the Red Hat Network registration process is used to create a System Profile, which is essential to receiving update notifications about your system. When satisfied, click **Forward**.

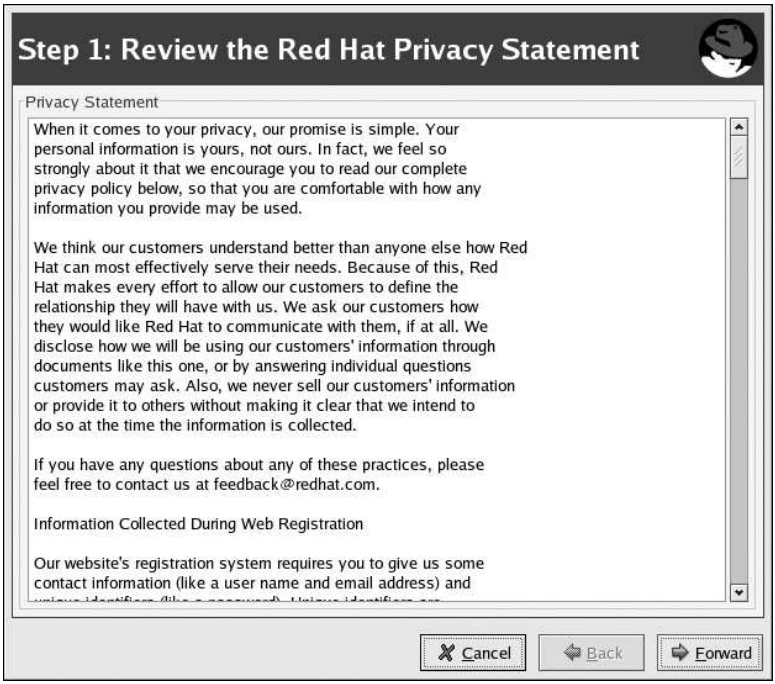
Step 1: Review the Red Hat Privacy Statement
Privacy Statement
When it comes to your privacy, our promise is simple. Your personal information is yours, not ours. In fact, we feel so strongly about it that we encourage you to read our complete privacy policy below, so that you are comfortable with how any information you provide may be used.
We think our customers understand better than anyone else how Red Hat can most effectively serve their needs. Because of this, Red Hat makes every effort to allow our customers to define the relationship they will have with us. We ask our customers how they would like Red Hat to communicate with them, if at all. We disclose how we will be using our customers' information through documents like this one, or by answering individual questions customers may ask. Also, we never sell our customers' information or provide it to others without making it clear that we intend to do so at the time the information is collected.
If you have any questions about any of these practices, please feel free to contact us at feedback@redhat.com.
Information Collected During Web Registration
Our website's registration system requires you to give us some contact information (like a user name and email address) and
Cancel
Back
Forward

**Figure 2-4. Red Hat Privacy Statement**

### 2.2.1. Registering a User Account

Before you can create a System Profile, you must create a user account. Red Hat recommends you create your account through the RHN website, but you may also do so through `up2date`. All that is required is a unique username-password combination and a valid email address.

In the screen shown in Figure 2-5, choose a username and password. Once logged in to Red Hat Network, you can modify your preferences, view your existing System Profile, or obtain the latest Red Hat software packages.

**Note**

If you are already a member of redhat.com, you can and should use the same username and password. However, you will still need to continue with the registration process to create your System Profile.

Your username has the following restrictions:

- Cannot contain any spaces
- Cannot contain the characters &, +, %, or ’

- Is not case-sensitive, thereby eliminating the possibility of duplicate usernames differing only by capitalization

In addition, the following restrictions apply to both your username and password:

- Must be at least four characters long
- Cannot contain any tabs
- Cannot contain any line feeds

Passwords are case-sensitive for obvious reasons.

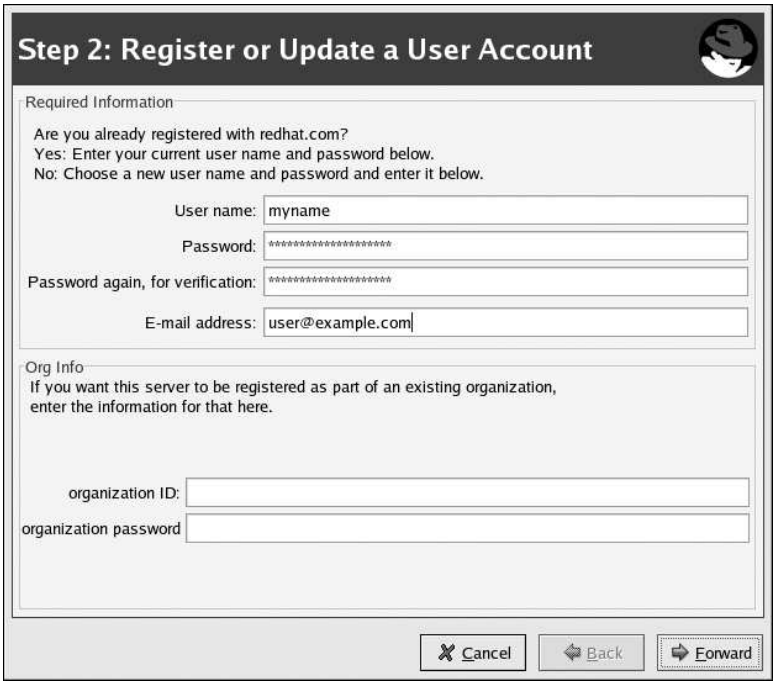
Step 2: Register or Update a User Account
Required Information
Are you already registered with redhat.com?
Yes: Enter your current user name and password below.
No: Choose a new user name and password and enter it below.
User name:
myname
Password:
Password again, for verification:
E-mail address:
user@example.com
Org Info
If you want this server to be registered as part of an existing organization,
enter the information for that here.
organization ID:
organization password
Cancel
Back
Forward

**Figure 2-5. Create a User Account**

You must choose a unique username. If you enter one already in use, you will see an error message (see Figure 2-6). Try different usernames until you find one that has not been used.

**Warning**

Be sure to identify a username that you will be satisfied with permanently, as this cannot be changed after account creation.

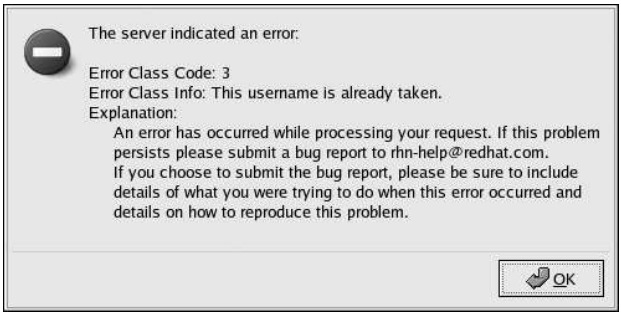
The server indicated an error:
Error Class Code: 3
Error Class Info: This username is already taken.
Explanation:
An error has occurred while processing your request. If this problem persists please submit a bug report to rhn-help@redhat.com.
If you choose to submit the bug report, please be sure to include details of what you were trying to do when this error occurred and details on how to reproduce this problem.
OK

**Figure 2-6. Error: Username Already Exists**

Most users can leave the **Org Info** section blank. If you have an existing organization account, enter your organization's ID and password in the provided text fields. If the values are valid, the system will be added to the organization's Red Hat Network account.

If you have already registered a machine and created a System Profile, you can add a new machine to your account. Run the **Red Hat Update Agent** on the new machine you wish to add, and enter your existing Red Hat Network username and password. The new machine will be added to your existing account, and you can log into Red Hat Network with your username and password to view all your systems simultaneously.

In the Create Account screen, click **Forward** to continue.

If you are a new user to RHN, the **Red Hat Update Agent** takes you to the screen shown in Figure 2-7. Here you will add details about yourself and your business, if applicable, and identify the methods by which you should be reached.

**Note**

Unlike other details, your company name can be changed only through Red Hat Customer Service, so enter it carefully. If you do need to have your company name changed, send your request to customerservice@redhat.com.

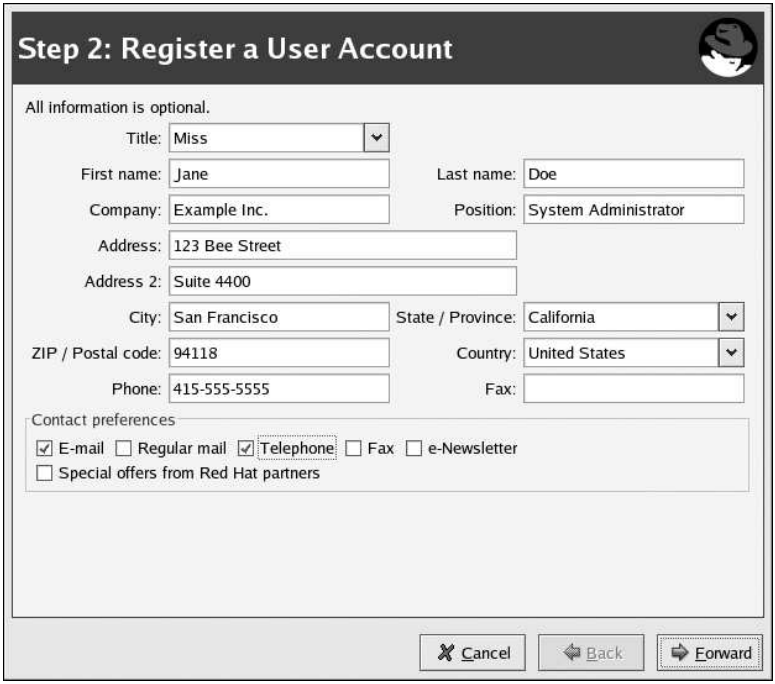


**Figure 2-7. Register a User Account**

Once satsfied with the information supplied, click **Forward** to continue.

## 2.2.2. Registering a System Profile

Now that you have a user account, you can create a System Profile that consists of hardware and software information about your Red Hat Enterprise Linux system. The System Profile information is used by Red Hat Network to determine what software update notifications you receive.

### 2.2.2.1. Hardware System Profile

After creating a username and password for your Red Hat Network account, the **Red Hat Update Agent** probes your system for the following information:

- Red Hat Linux version
- Hostname
- IP address
- CPU model
- CPU speed
- Amount of RAM
- PCI devices

- Disk sizes
- Mount points

The next step is choosing a profile name for your system as shown in Figure 2-8. The default value is the hostname for the system. You may modify this to be a more descriptive string, such as **`Email Server for Support Team`**, if you find it more helpful. Optionally, you can enter a computer serial or identification number for the system.

If you do not wish to include information about your hardware or network in your System Profile, deselect **Include information about hardware and network** (see Figure 2-8).

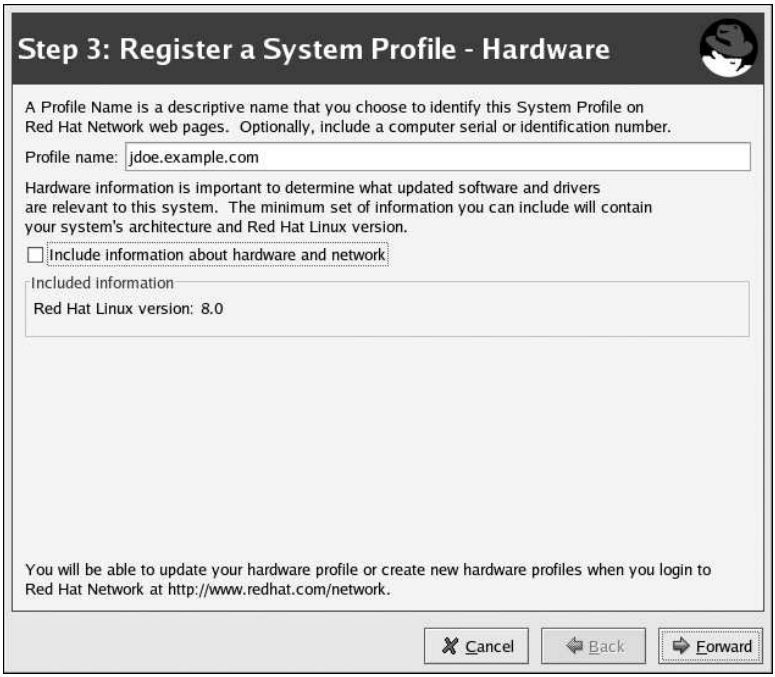
Step 3: Register a System Profile - Hardware
A Profile Name is a descriptive name that you choose to identify this System Profile on Red Hat Network web pages. Optionally, include a computer serial or identification number.
Profile name: jdoe.example.com
Hardware information is important to determine what updated software and drivers are relevant to this system. The minimum set of information you can include will contain your system's architecture and Red Hat Linux version.
Include information about hardware and network
Included information
Red Hat Linux version: 8.0
You will be able to update your hardware profile or create new hardware profiles when you login to Red Hat Network at http://www.redhat.com/network.
Cancel
Back
Forward

**Figure 2-8. System Profile - Hardware**

Click **Forward** to continue with the registration process.

### 2.2.2.2. Software System Profile

The software System Profile consists of a list of RPM packages for which you wish to receive notifications. The **Red Hat Update Agent** shows you a list of all RPM packages listed in the RPM database on your system and then allows you to customize the list by deselecting packages.

#### *2.2.2.2.1. Gathering RPM Database Information*

Only those packages you choose during this part of the registration will be included in your System Profile, and you will receive notifications only about the packages in your System Profile. Therefore,

you must include packages in your profile to have RHN send you Errata regarding them. You should also note if you use an older version of a package and deselect it from the list, it will not be replaced with a newer version.

This RPM list can be modified through the Red Hat Network Web interface or by using the **Red Hat Update Agent**. Figure 2-9 shows the progress bar you will see while the **Red Hat Update Agent** gathers a list of the RPM packages installed on your system. This operation may take some time, depending on your system installation.

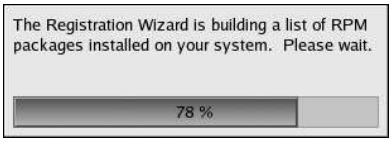


**Figure 2-9. Registration Wizard**

Once the RPM package list is built, the list will be displayed as shown in Figure 2-10. Deselecting **Include RPM Packages installed on this system in my System Profile** will omit this information from your System Profile.

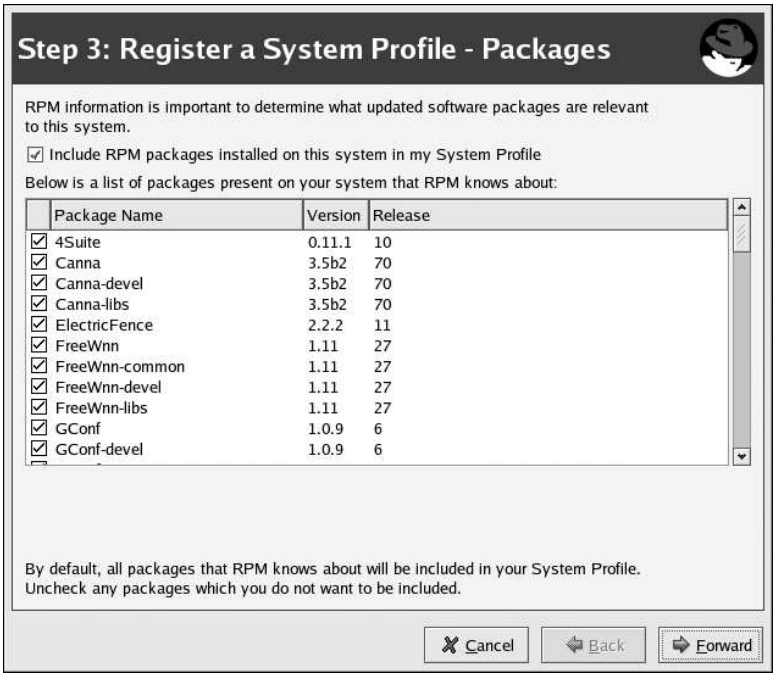
Step 3: Register a System Profile - Packages
RPM information is important to determine what updated software packages are relevant to this system.
Include RPM packages installed on this system in my System Profile
Below is a list of packages present on your system that RPM knows about:
Package Name Version Release
4Suite 0.11.1 10
Canna 3.5b2 70
Canna-devel 3.5b2 70
Canna-libs 3.5b2 70
ElectricFence 2.2.2 11
FreeWnn 1.11 27
FreeWnn-common 1.11 27
FreeWnn-devel 1.11 27
FreeWnn-libs 1.11 27
GConf 1.0.9 6
GConf-devel 1.0.9 6
By default, all packages that RPM knows about will be included in your System Profile.
Uncheck any packages which you do not want to be included.
Cancel
Back
Forward

**Figure 2-10. RPM Package Information**

#### *2.2.2.2.2. Choosing RPM Packages to Exclude from the System Profile*

By default, all RPM packages in your RPM database are included in your System Profile to be updated by Red Hat Network. To exclude a package, uncheck the package from the list by clicking the check-box beside the package name. For example, Figure 2-11 shows that the **Canna-devel** and **Canna-libs** packages have been omitted from the package list.

Choose which packages to exclude, if any, from the System Profile, and click **Forward** to continue with the registration process.

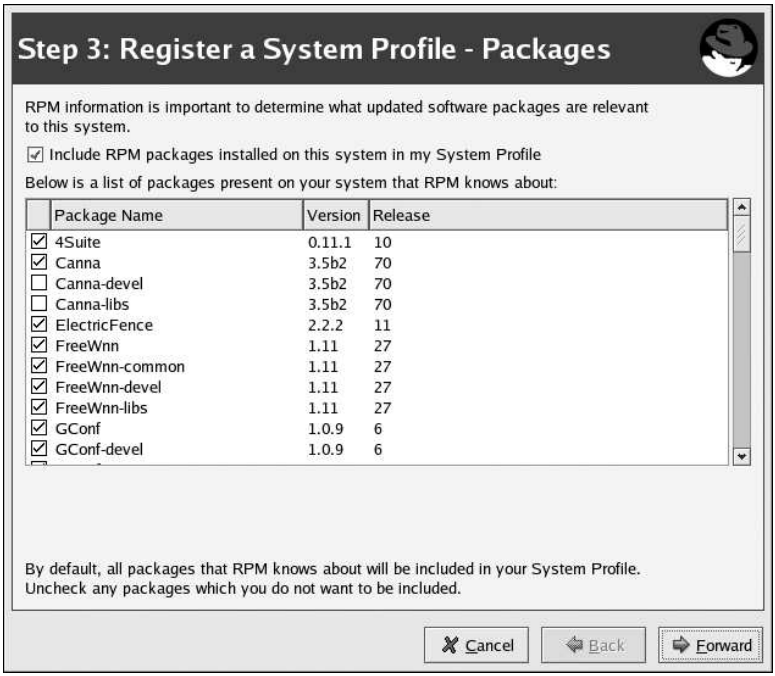
Step 3: Register a System Profile - Packages
RPM information is important to determine what updated software packages are relevant to this system.
Include RPM packages installed on this system in my System Profile
Below is a list of packages present on your system that RPM knows about:
Package Name
Version
Release
4Suite 0.11.1 10
Canna 3.5b2 70
Canna-devel 3.5b2 70
Canna-libs 3.5b2 70
ElectricFence 2.2.2 11
FreeWnn 1.11 27
FreeWnn-common 1.11 27
FreeWnn-devel 1.11 27
FreeWnn-libs 1.11 27
GConf 1.0.9 6
GConf-devel 1.0.9 6
By default, all packages that RPM knows about will be included in your System Profile.
Uncheck any packages which you do not want to be included.
Cancel
Back
Forward

**Figure 2-11. Choose which RPM Packages to Exclude from System Profile**

### 2.2.2.3. Finishing Registration

As seen in Figure 2-12, the last step of registration is to confirm that you want to send your System Profile to the Red Hat Network. If you choose **Cancel** at this point, no information will be sent. Clicking **Forward** will submit your RHN System Profile.

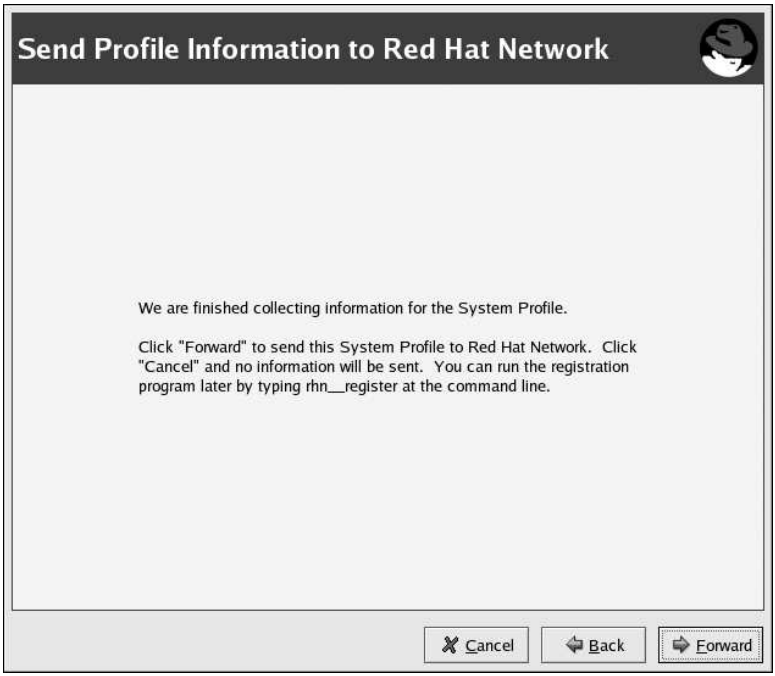
Send Profile Information to Red Hat Network
We are finished collecting information for the System Profile.
Click "Forward" to send this System Profile to Red Hat Network. Click "Cancel" and no information will be sent. You can run the registration program later by typing rhn_register at the command line.
Cancel
Back
Forward

**Figure 2-12. Finished Collecting Information for System Profile**

Figure 2-13 shows the progress bar you will see while your profile is being sent. This process may take some time depending on your connection speed.

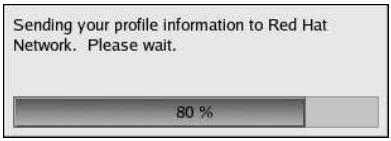


**Figure 2-13. Send System Profile to Red Hat Network**

You will know your System Profile has been successfully sent when you see the **Channels** screen (Figure 2-14) appear. Refer to Section 2.3.1 *Choosing a Software Channel* for continued instructions.

## 2.3. Setup and Use

After completing the registration process, you should set up the **Red Hat Update Agent** to effectively manage all of your system's package updates. This requires selecting its channel, identifying the packages requiring maintenance, and making your first installation.

Before you proceed, however, you should consider ensuring you have the latest version of the **Red Hat Update Agent**, as development on it is continuous. This task is as simple as running the tool against its own package. Shut down the GUI version and run this command in a terminal (as root), like so:

```
up2date up2date
```

### 2.3.1. Choosing a Software Channel

The first step is to select the channel from which you want the updated packages to be retrieved. After you send your System Profile, the **Channels** screen (Figure 2-14) appears. Select the appropriate base channel and click **Forward** to continue. The **Red Hat Update Agent** offers only the channels enabled for the system in RHN (or your RHN Satellite Server). Refer to Section 6.6 *Channels* for more information on channels and how channels are used to determine which packages are installed.

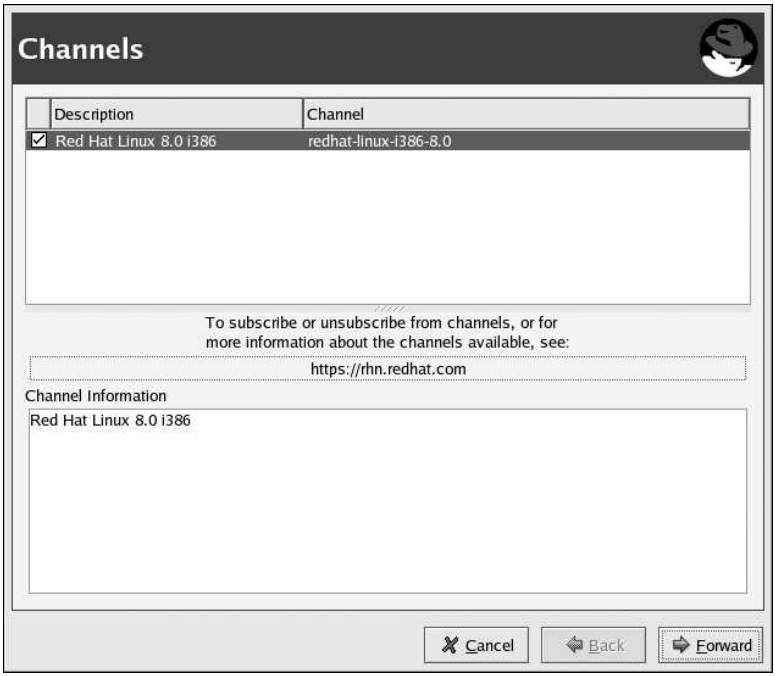


**Figure 2-14. Channels**

### 2.3.2. Choosing Packages to Update

After clicking **Forward**, the dialog box in Figure 2-15 will appear. This means a connection to Red Hat Network is being established and your customized list of updates is being retrieved. This might take some time, depending on the speed of your connection and the number of packages you have installed.

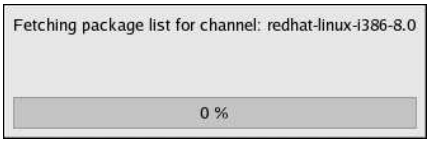


**Figure 2-15. Retrieve Update Information**

While you see this dialog box, the **Red Hat Update Agent** uses your unique Digital Certificate (`/etc/sysconfig/rhn/systemid`) to determine if there are any updated packages available for your system. If there are no updated packages available for your system, the dialog box in Figure 2-16 appears. Click **OK** to exit the **Red Hat Update Agent**.

**Figure 2-16. No new packages needed**

If you excluded any packages while registering your System Profile, these are displayed in Figure 2-17. You may override these settings and include any of these packages in the update by selecting the checkboxes next to them. To see a summary of each package in the **Package Information** section at the bottom of the screen, click the name of the package.

Packages Flagged to be Skipped
Select all packages
Package Name
Version
Rel.
Arch
Size
Reason Skipped
kernel 2.4.18 19.8.0 i686 13322 kE Pkg name/pattern
kernel-BOOT 2.4.18 19.8.0 i386 6144 kB Pkg name/pattern
kernel-bigmem 2.4.18 19.8.0 i686 13818 kE Pkg name/pattern
kernel-debug 2.4.18 19.8.0 i686 13581 kE Pkg name/pattern
kernel-doc 2.4.18 19.8.0 i386 1756 kB Pkg name/pattern
kernel-smp 2.4.18 19.8.0 i686 13836 kE Pkg name/pattern
Package Information
View Advisory
The Linux kernel (the core of the Linux operating system).
The kernel package contains the Linux kernel (vmlinuz), the core of the Red Hat Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.
According to your preferences you have chosen not to automatically update the above packages. If you would like to override your settings and include one of the above packages in the list of packages to retrieve, select its checkbox.
Cancel
Back
Forward

**Figure 2-17. Packages Flagged to be Skipped**

If you want to view the advisory for the RPM Alert, click the **View Advisory** button. This will display what type of Errata Alert it is and what problem(s) it addresses as shown in Figure 2-18. Click **OK** to close the advisory. Click **Finished** when you are finished selecting packages to include.

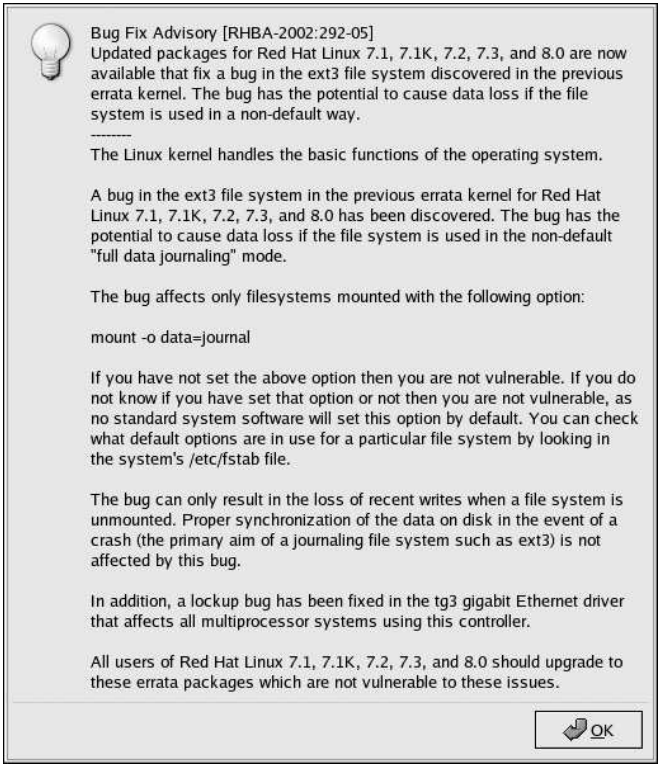
Bug Fix Advisory [RHBA-2002:292-05]
Updated packages for Red Hat Linux 7.1, 7.1K, 7.2, 7.3, and 8.0 are now available that fix a bug in the ext3 file system discovered in the previous errata kernel. The bug has the potential to cause data loss if the file system is used in a non-default way.
--------
The Linux kernel handles the basic functions of the operating system.
A bug in the ext3 file system in the previous errata kernel for Red Hat Linux 7.1, 7.1K, 7.2, 7.3, and 8.0 has been discovered. The bug has the potential to cause data loss if the file system is used in the non-default "full data journaling" mode.
The bug affects only filesystems mounted with the following option:
mount -o data=journal
If you have not set the above option then you are not vulnerable. If you do not know if you have set that option or not then you are not vulnerable, as no standard system software will set this option by default. You can check what default options are in use for a particular file system by looking in the system's /etc/fstab file.
The bug can only result in the loss of recent writes when a file system is unmounted. Proper synchronization of the data on disk in the event of a crash (the primary aim of a journaling file system such as ext3) is not affected by this bug.
In addition, a lockup bug has been fixed in the tg3 gigabit Ethernet driver that affects all multiprocessor systems using this controller.
All users of Red Hat Linux 7.1, 7.1K, 7.2, 7.3, and 8.0 should upgrade to these errata packages which are not vulnerable to these issues.
OK

**Figure 2-18. View Advisory**

The **Available Package Updates** screen is the next to appear. If your system is not up-to-date, your customized list of available updated packages is displayed as shown in Figure 2-19.

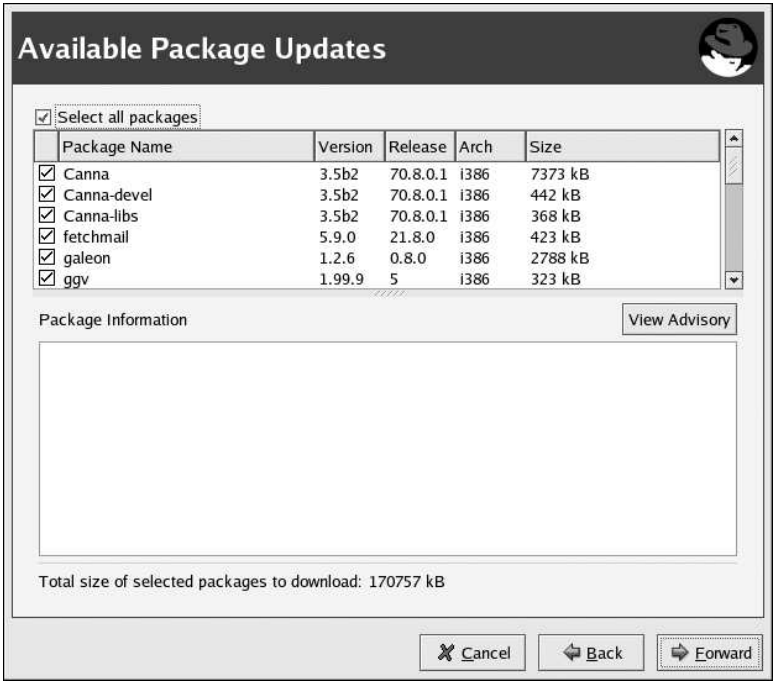


**Figure 2-19. List of Available Updates**

By default, no packages are selected for download. To select a package for download (and installation, if you chose that option), click its checkbox. To select all the packages listed, click the checkbox next to **Select all packages**.

After choosing which packages to update, the **Red Hat Update Agent** tests for RPM dependencies and prompts you if you have chosen to omit packages that are required for software updates that you did choose. The dialog box in Figure 2-20 is shown while it is testing for dependencies. This process might take some time depending upon how many packages are updating.

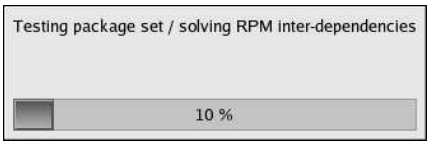


**Figure 2-20. Testing Packages**

After testing is complete, package retrieval begins. The progress of each package retrieval is shown in Figure 2-21. When they have all been retrieved, the message **All finished** is displayed at the bottom of the screen. Click **Forward** to continue.

Retrieving Packages
Retrieving: xinetd-2.3.7-5.i386.rpm
A secure replacement for inetd.
Xinetd is a secure replacement for inetd, the Internet services daemon. Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files are located in the /etc/xinetd.d directory.
209 of 209 kB transferred at 94 kB/sec
Package transfer time: 00:00:02 (00:00:00 remaining)
100 %
Total progress:
100 %
All finished. Click "Forward" to continue.
Cancel
Back
Forward

**Figure 2-21. Retrieval Finished**

### 2.3.3. Installing Updated Packages

After downloading the packages through the **Red Hat Update Agent**, they must be installed. If you chose not to have the packages installed via the **Red Hat Update Agent**, skip to Section 2.3.5.2 *Manual Package Installation* for further instructions. If you configured it to install the packages (the default setting), the selected packages are installed. The progress of installing each package, as well as the total progress, is displayed. When the packages have been installed, as seen in Figure 2-22, click **Forward** to continue.

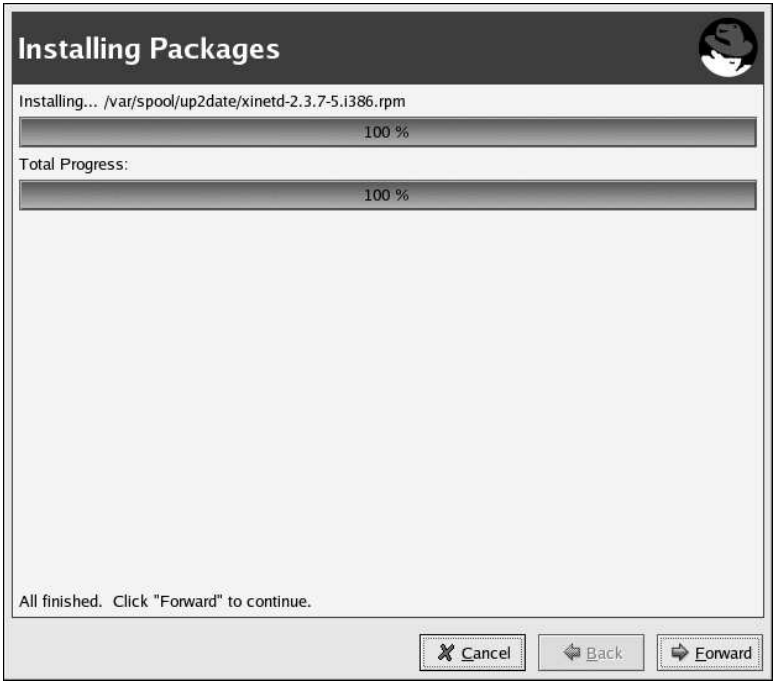


**Figure 2-22. Installation Finished**

### 2.3.4. Update Agent Finished

When the **Red Hat Update Agent** has finished downloading the desired packages (and installing them if you chose the install option), you will see the screen in Figure 2-23. Click **Finish** to exit the **Red Hat Update Agent**.

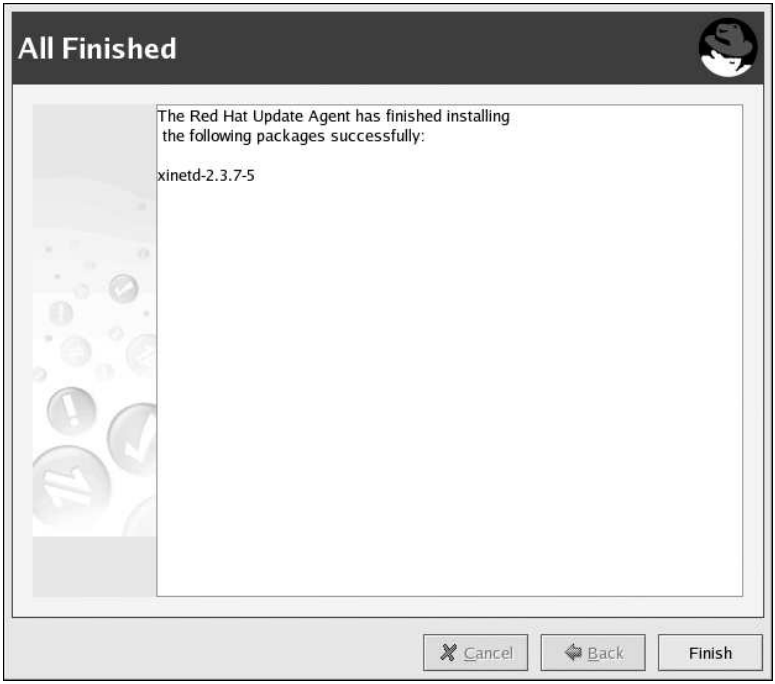


**Figure 2-23. Update Agent Finished**

### 2.3.5. Command Line Version

If you are not running X, you can still run the **Red Hat Update Agent** from a virtual console or remote terminal. If you are running X but want to use the command line version, you can force it not to display the graphical interface with the following command:

```
up2date --nox
```

The command line version of the **Red Hat Update Agent** allows you to perform advanced functions or to perform actions with little or no interaction. For example, the following command updates your system with no interaction. It will download the newer packages and install them if you configured it to install them.

```
up2date -u
```

The command line version of the **Red Hat Update Agent** accepts the following arguments:

| Argument | Description |
|---|---|
| `-?`, `--usage` | Briefly describe the available options. |
| `-h`, `--help` | List the available options and exit. |

| Argument | Description |
|---|---|
| `--arch=`*`architecture`* | Force `up2date` to install this architecture of the package. Not valid with `--update`, `--list`, or `--dry-run`. |
| `--channel=`*`channel`* | Specify which channels to update from using channel labels. |
| `--configure` | Configure **Red Hat Update Agent** options. Refer to Section 2.4 *Configuration* for detailed instructions. |
| `-d`, `--download` | Download packages only; do not install them. This argument temporarily overrides the configuration option **Do not install packages after retrieval.** Use this option if you prefer to install the packages manually. |
| `--dbpath=`*`dir`* | Specify an alternate RPM database to use temporarily. |
| `--dry-run` | Do everything but download and install packages. This is useful in checking dependencies and other requirements prior to actual installation. |
| `-f`, `--force` | Force package installation. This option temporarily overrides the file, package, and configuration skip lists. |
| `--firstboot` | Pop up in the center of the screen for Firstboot. |
| `--get` | Fetch the package specified without resolving dependencies. |
| `--get-source` | Fetch the source package specified without resolving dependencies. |
| `--gpg-flags` | Show the flags GPG will be invoked with, such as the keyring. |
| `--hardware` | Update this system's hardware profile on RHN. |
| `-i`, `--install` | Install packages after they are downloaded. This argument temporarily overrides the configuration option **Do not install packages after retrieval.** |
| `--installall` | Install all available packages. Used with `--channel`. |
| `--justdb` | Only add packages to the database and do not install them. |
| `-k`, `--packagedir` | Specify a colon-separated path of directories to look for packages in before trying to download them. |
| `-l`, `--list` | List packages relevant to the system. |
| `--list-rollbacks` | Show the package rollbacks available. |
| `--nodownload` | Do not download packages at all. This is useful in testing. |
| `--nosig` | Do not use GPG to check package signatures. This option temporarily overrides the saved configuration option. |
| `--nosrc` | Do not download source packages (SRPMs). |
| `--nox` | Do not attempt to run in X. This launches the command line version of the **Red Hat Update Agent**. |
| `-p`, `--packages` | Update packages associated with this System Profile. |
| `--proxy=`*`proxy URL`* | Specify an HTTP proxy to use. |
| `--proxyPassword=`*`proxy password`* | Specify a password to use with an authenticated HTTP proxy. |

| Argument | Description |
|---|---|
| `--proxyUser=`*`proxy user ID`* | Specify a username to use with an authenticated HTTP proxy. |
| `--register` | Register (or re-register) this system with RHN. Refer to Section 2.2 *Registration* for detailed instructions. |
| `--serverUrl=`*`server URL`* | Specify an alternate server from which to retrieve packages. |
| `--showall` | List all packages available for download. |
| `--show-available` | List all packages available that are not currently installed. |
| `--show-channels` | Show the channel name associated with each package. |
| `--show-orphans` | List all packages currently installed that are not in channels the system is subscribed to. |
| `--show-package-dialog` | Show the package installation dialog in GUI mode. |
| `--solvedeps=`*`dependencies`* | Find, download, and install the packages necessary to resolve dependencies. |
| `--src` | Download source packages, as well as binary RPMs. |
| `--tmpdir=`*`directory`* | Temporarily override the configured package directory. The default location is `/var/spool/up2date`. This option is useful if you do not have enough space in the configured location. |
| `--undo` | Reverse the last package set update. |
| `-u`, `--update` | Update system with all relevant packages. |
| `--upgrade-to-release=`*`release version`* | Upgrade to the channel specified. |
| `--uuid=`*`uuid`* | Pass in a Unique User ID generated by the Alert Notification tool. |
| `-v`, `--verbose` | Show additional output while updating. |
| `--version` | Show `up2date` version information. |
| `--whatprovides=`*`dependencies`* | Show the packages that resolve the comma-separated list of dependencies. |

**Table 2-2. Update Agent Command Line Arguments**

#### 2.3.5.1. Installing the Red Hat GPG key

The first time you run the graphical version of the **Red Hat Update Agent**, it prompts you to install the Red Hat GPG key. This key is required to authenticate the packages downloaded from Red Hat Network. If you run the command line version the first time you start **Red Hat Update Agent**, you need to install the Red Hat GPG key manually. If you do not have it installed, you will see the following message:

```
Your GPG keyring does not contain the Red Hat, Inc. public key.
Without it, you will be unable to verify that packages Update Agent downloads
are securely signed by Red Hat.
```

**Note**

GPG keys must be installed for each user. To install the key to use with Red Hat Network, import the key while logged in as root.

The method for installing the key varies depending on your version of RPM. Starting with version 4.1, which shipped with Red Hat Enterprise Linux 3, you may import GPG keys using `rpm`, like so (as root):

```
rpm --import /usr/share/doc/rpm-4.1/RPM-GPG-KEY
```

For older versions of RPM, such as the one that came with Red Hat Enterprise Linux 2.1, use the `gpg` command (as root):

```
/usr/bin/gpg --import /usr/share/rhn/RPM-GPG-KEY
```

If you need to download the Red Hat GPG key first, you may obtain it from https://www.redhat.com/security/team/key.html . Here's an example:

```
Type bits/keyID Date User ID
pub  1024D/650D5882 2001-11-21 Red Hat, Inc. (Security Response Team)
sub  2048g/7EAB9AFD 2001-11-21

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (GNU/Linux)

mQGiBDv70vQRBADh701rf8WUzDG88kqlV/N5KQ1PF0amnODB/1EeuAD7n6bCBRmV
ekQWJCdfab0Rf1S+VsFg6IAAAmDIarVnacTLQzqCdGJqTpXm/rGVpLv+mCh+OmT9
QRFbjSzB0uPJOpiIvJwSS00D/wJ8XKzHkVNgW3DiJ9Qz2BHYszU2ISI6FwCgxY6d
IVjWT5jblkLNjtD3+fR024ED/i0e2knetTX3S9LjC+HdGvP8Eds92Ti2CnJLaFJk
Rp749PucnK9mzxPcO2jSHgdtjWAXst/st+gWFVbFmkjBQDVSd00B/xEwIlT1+LN8
V7R8BElBmg99IlJmDvA2BI/seXvafhzly9bxSHScFnceco/Az9umIs3NXwv3/yOm
ZakDBAC6SAGHBmpVkOdeXJDdb4LcbEhErFU3CpRCjZ6AOnFuiVlMGdulZXvEUgBA
I6/PDE5nBHfZY3zPjyLPZVtgYioJpZqcRIx/g+bX2O8kPqvJEuZ19tLCdykfZGpy
bsV7QdSGqBk3snNOizmFj543RaHyEbnwKWbNADhujWMeUAxN+7Q8UmVkIEhhdCwg
SW5jLiAoU2VjdXJpdHkgUmVzcG9uc2UgVGVhbSkgPHNlY2FsZXJ0QHJlZGhhdC5j
b20+iFcEExECABcFAj3GczYFCwcKAwQDFQMCAxYCAQIXgAAKCRBeVICDZQ1YghAU
AJoCeQfuMR2dKyLft/10O6qUs+MNLQCggJgdO8MUO2y11TWID3XOYgyQG+2InAQT
AQIABgUCPtyYpQAKCRDurUz9SaVj2e97A/0b2s7OhhAM1jNwMQS4I2UWVGbgtxdu
D+yBcG/3mwL76MJVY7aX+NN/tT9yDGU+FSiQZZCL/4OFOHMvjpcDqfJY+zpTlBii
ZMAPJWTs2bB+0QaXxUgWlwW84GVf2rA6RSbvMLTbDjTH8t7J1RGP9zAqu8SgraTA
QbQdao6TNxVt+ohGBBMRAgAGBQI+3LjCAAoJECGRgM3bQqYOf5MAoIjiJDe+hDOj
9+jlR0qDs9lIi/C2AJ9SBBfd4A8hyR4z3lY7e0LzjWF51LkCDQQ7+9O3EAgA8tMs
xdUmuTfA+X78fMXh7LCvrL4Hi28CqvNM+Au81XJjDLNawZvpVmFlMmd9h0Xb5Jt2
BZWLR13rcDUByNdw1EWhVAzCz6Bp9Z3MIDhcP00iIBctIHn7YP9fi5vV0G03iryT
XE01mhWoBlC233wr3XHwsqxFfZzaCZqqNKTl0+PNfEAIzJRgtYiW8nzFTPpIR05E
oRn6EvmQfayOF2uYDX9Sk//lOD7T7RLtKjM/hPW/9NoCGwwROaG+VUzVv4aelh1L
dJGEjpFtdxcrOUMD8xbkuGMznu0mpDI+J2BUDh5n57yOyEMaGrQ0jfY1ZqdqDvZg
osY1ZHa6KlmuCWNTnwADBQf/XYhCicp6iLetnPv6lYtyRfFRpnK98w3br+fThywC
t81P2nKv8lio6OsRbksGc1gX8Zl6GoHQYfDe7hYsCHZPoWErobECFds5E9M7cmzV
TTyNTvrELrs07jyuPb4Q+mHcsYPILGR3M+rnXKGjloz+05kOPRJaBEBzP6B8SZKy
QNqEfTkTYU4Rbhkzz/UxUxZoRZ+tqVjNbPKFpRraiQrUDsZFbgksBCzkzd0YURvi
CegO2K7JPKbZJo6eJA10qiBQvAx2EUijZfxIKqZeLx40EKMaL7Wa2CM/xmkQmCgg
Hyu5bmLSMZ7cxFSWyXOst78dehCKv9WyPxHV3m4iANWFL4hGBBgRAgAGBQI7+9O3
AAoJEF5UgINlDViCKWcAoMCeYStWVKXJTytzHEL6Wl8rXr8WAKCHuapJIA4/eFsf
4ciWtjY8cO0v8Q==
```

```
=yOVZ
-----END PGP PUBLIC KEY BLOCK-----
```

Save the text file and import it into your keyring using the method applicable for your version of RPM.

#### 2.3.5.2. Manual Package Installation

If you chose to download the software updates with the **Red Hat Update Agent** or from the RHN website, you must install them manually using RPM.

To install them, change to the directory that contains the downloaded packages. The default directory is `/var/spool/up2date`. Then, type the command `rpm -Uvh *.rpm`. When the packages are finished installing, you can delete them if you wish. You do not need them anymore.

After installing the packages, you must update your System Profile so that you are not prompted to download them again. Refer to Section 2.3.5.3 *Synchronizing Your System Profile* for details.

#### 2.3.5.3. Synchronizing Your System Profile

If you configured the **Red Hat Update Agent** to install the latest packages, then your System Profile stored by Red Hat Network will be updated after the packages are installed. However, if you only download the latest RPM packages using the **Red Hat Update Agent**, download the RPM packages from the website, or upgrade/install/remove RPM packages yourself, your System Profile will not be updated automatically. You will need to send your updated System Profile to the RHN Servers.

To synchronize the RPM package list on your local system and on Red Hat Network, run the command:

```
up2date -p
```

After running this command, your RHN System Profile will reflect the latest software versions installed on your system.

#### 2.3.5.4. Log File

The **Red Hat Update Agent** keeps a log of all the actions that it performs on your system in the file `/var/log/up2date`. It uses the standard rotating log method. Thus, older logs are in `/var/log/up2date.1`, `/var/log/up2date.2`, and `/var/log/up2date.3`. The log files store actions performed by the **Red Hat Update Agent** such as when your RPM database is opened, when it connects to Red Hat Network to retrieve information from your System Profile, which packages are downloaded, which packages are installed using the **Red Hat Update Agent**, and which packages are deleted from your system after installation. If you choose to install and delete packages yourself, it will not be logged in this file. You should keep your own log of actions not performed with the **Red Hat Update Agent**.

## 2.4. Configuration

The **Red Hat Update Agent** offers various options to configure its settings.

If you are not running the X Window System or prefer the command line version, skip to Section 2.4.2 *Command Line Version*.

### 2.4.1. Using the Red Hat Update Agent Configuration Tool

You must be root to run the **Red Hat Update Agent Configuration Tool**. If you start the **Red Hat Update Agent Configuration Tool** as a standard user, you will be prompted to enter the root password before proceeding. The **Red Hat Update Agent Configuration Tool** can be started by typing the command `up2date-config` at a shell prompt (for example, an xterm or a gnome-terminal).

#### 2.4.1.1. General Settings

The **General** tab allows you to enable an HTTP Proxy Server. If your network connection requires you to use an HTTP Proxy Server to make HTTP connections, select the **Enable HTTP Proxy** option and type your proxy server in the text field with the format http://HOST:PORT. For example, to use the proxy server http://squid.mysite.org on port 3128, you would enter **`http://squid.mysite.org:3128`** in the text field. Additionally, if your proxy server requires a username and password, select the **Use Authentication** option and enter your username and password in the respective text fields.

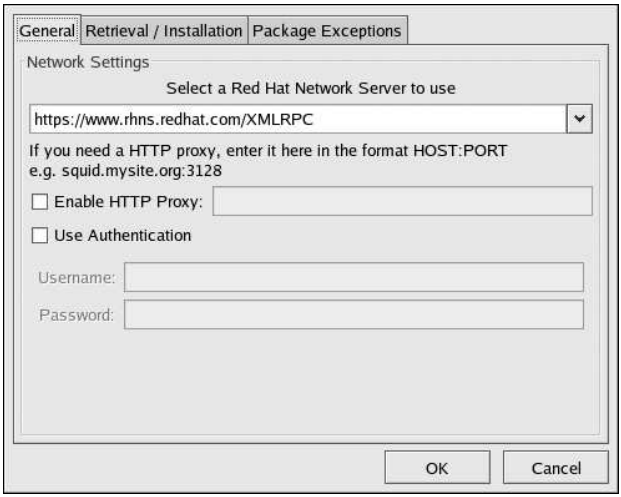


**Figure 2-24. General Settings**

In addition, RHN Proxy and Satellite customers have the option of selecting Red Hat Network Servers here. These customers should refer to the RHN Client Configuration Guide for detailed instructions.

#### 2.4.1.2. Retrieval/Installation Settings

The **Retrieval/Installation** tab allows you to customize your software package retrieval and package installation preferences.

**Warning**

You must use **Red Hat Update Agent** Version 2.5.4 or higher to upgrade your kernel automatically. **Red Hat Update Agent** will install the updated kernel and configure LILO or GRUB to boot the new kernel the next time the system is rebooted.

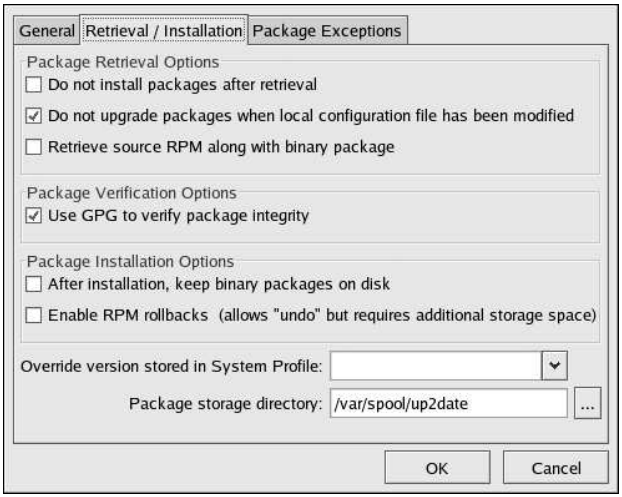
General
Retrieval / Installation
Package Exceptions
Package Retrieval Options
Do not install packages after retrieval
Do not upgrade packages when local configuration file has been modified
Retrieve source RPM along with binary package
Package Verification Options
Use GPG to verify package integrity
Package Installation Options
After installation, keep binary packages on disk
Enable RPM rollbacks (allows "undo" but requires additional storage space)
Override version stored in System Profile:
Package storage directory:
/var/spool/up2date
...
OK
Cancel

**Figure 2-25. Retrieval/Installation Settings**

The following package retrieval options can be selected (see Figure 2-25):

- **Do not install packages after retrieval** — download selected RPM packages to desired directory and ignore the installation preferences
- **Do not upgrade packages when local configuration file has been modified** — if the configuration file has been modified for a package such as `apache` or `squid`, do not attemp to upgrade it. This option is useful if you are installing custom RPMs on your system and you do not want them updated or reverted to the default Red Hat Enterprise Linux packages.
- **Retrieve source RPM along with binary package** — download both the source (`*.src.rpm`) and the binary (`*.[architecture].rpm`) files

The following installation options are configurable (see Figure 2-25):

- **Use GPG to verify package integrity** — before installing the packages, verify Red Hat's GPG signature (highly recommended for security reasons)
- **After installation, keep binary packages on disk** — save binary packages in desired directory instead of deleting them after installation

The following additional options are configurable from this tab:

- **Override version stored in System Profile** — override the Red Hat Linux version in your System Profile
- **Package storage directory** — change the directory where packages are downloaded; the default location is `/var/spool/up2date`

#### 2.4.1.3. Package Exceptions Settings

The **Package Exceptions** tab allows you to define which packages to exclude from the list of updated RPM packages according to the package name or file name (see Figure 2-26).

To define a set of packages to be excluded according to the package name, enter a character string including wild cards (*) in the **Add new** text field under in the **Package Names to Skip** section. A wild card at the end of the character string means all packages beginning with the character string will be excluded from the list. A wild card at the beginning of the character string means any packages that end with the character string will be excluded from the list.

For example, if the string **kernel*** in the **Package Names to Skip** section, the **Red Hat Update Agent** will not display any packages beginning with kernel.

To exclude packages by file name, follow the same rules except click the **Add** button next to the **File Names to Skip** section.

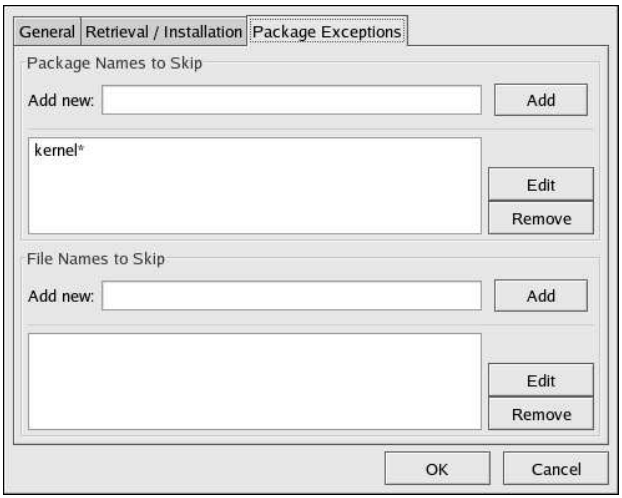


**Figure 2-26. Package Exceptions Settings**

### 2.4.2. Command Line Version

The command line version of this tool performs the same function as the graphical version. It allows you to configure the settings used by the **Red Hat Update Agent** and store them in the configuration file `/etc/sysconfig/rhn/up2date`.

To run the command line version of the **Red Hat Update Agent Configuration Tool**, use the following command:

```
up2date --nox --configure
```

You will be presented with a list of options and their current values:

```
0.  debug               No
1.  isatty              Yes
```

```
2.  depslist           []
3.  networkSetup       Yes
4.  retrieveOnly       No
5.  enableRollbacks    No
6.  pkgSkipList        ['kernel*']
7.  storageDir         /var/spool/up2date
8.  adminAddress       ['root@localhost']
9.  noBootLoader       No
10. serverURL          https://xmlrpc.rhn.redhat.com/XMLRPC
11. fileSkipList       []
12. sslCACert          /usr/share/rhn/RHNS-CA-CERT
13. noReplaceConfig    Yes
14. useNoSSLForPackage No
15. systemIdPath       /etc/sysconfig/rhn/systemid
16. enableProxyAuth    No
17. retrieveSource     No
18. versionOverride
19. headerFetchCount   10
20. networkRetries     5
21. enableProxy        No
22. proxyPassword
23. noSSLServerURL     http://xmlrpc.rhn.redhat.com/XMLRPC
24. keepAfterInstall   No
25. proxyUser
26. removeSkipList     ['kernel*']
27. useGPG             Yes
28. gpgKeyRing         /etc/sysconfig/rhn/up2date-keyring.gpg
29. httpProxy
30. headerCacheSize    40
31. forceInstall       No


Enter number of item to edit <return to exit, q to quit without saving>:
```

Enter the number of the item that you want to modify and enter a new value for the option. When you finish changing your configuration, press [Enter] to save your changes and exit. Press [q] and then [Enter] to quit without saving your changes.

**Important**

Although this isn't configurable, users should still make note that the port used by the **Red Hat Update Agent** is 443 for SSL (HTTPS) and 80 for non-SSL (HTTP). By default, `up2date` uses SSL only. For this reason, users should ensure their firewalls allow connections over port 443. To bypass SSL, in `/etc/sysconfig/rhn/up2date` change the protocol for `serverURL` from **`https`** to **`http`**.

## 2.5. Registering with Activation Keys

In addition, to the standard **Red Hat Update Agent** interface, `up2date` offers a utility aimed at batch processing the registration of systems: activation keys. Each unique key can be used to register Red Hat Enterprise Linux systems, entitle them to an RHN service level, and subscribe them to specific channels and system groups, all in one action.

Thus, channel and group subscriptions can be automated along with registration, thereby bypassing entitlement and registration through either the **Red Hat Network Registration Client** or the **Red Hat Update Agent**, both of which offer the activation keys utility `rhnreg_ks` as part of their packages.

**Note**

Systems running Red Hat Enterprise Linux 2.1 need version 2.9.3-1 or higher of the `rhn_register` package. It is highly recommended you obtain the latest version before using activation keys.

Before using an activation key, you must first generate one through the RHN website. Refer to Section 6.4.7 *Activation Keys* — for precise steps.

To use an activation key, as root from a shell prompt on the system to be registered, run the `rhnreg_ks` command followed by the key. For example:

```
rhnreg_ks --activationkey=7202f3b7d218cf59b764f9f6e9fa281b
```

Systems running Red Hat Enterprise Linux 2.1 will use the `--serialnumber` instead of `--activationkey`, like so:

```
rhnreg_ks --serialnumber=7202f3b7d218cf59b764f9f6e9fa281b
```

In addition, Provisioning-entitled systems may use multiple activation keys at once, either at the command line or within kickstart profiles, to include a variety of values without creating a special key for the desired results. To do this, specify the keys separated by commas, like this:

```
rhnreg_ks --activationkey=7202f3b7d218cf59b764f9f6e9fa281b,\
 39f41081f0329c20798876f37cb9p6a3
```

**Note**

The trailing backslash (`\`) in this command example is a continuation character; it may safely be omitted.

Refer to Section 6.4.7.2 *Using Multiple Activation Keys at Once* — to understand how differences in activation keys are handled.

This command performs all the actions of the **Red Hat Network Registration Client** and the registration function of the **Red Hat Update Agent**. Do not run either of these applications for registration after running `rhnreg_ks`.

A System Profile, including software and hardware information, is created for the system and sent to the RHN Servers along with the unique activation key. The system is registered with RHN under the account used to generate the key, entitled to an RHN service offering, and subscribed to the RHN channels and system groups selected during key generation. The system will not be subscribed to channels that contain packages not suitable for the system. For example, a Red Hat Enterprise Linux 2.1 system cannot be subscribed to the Red Hat Enterprise Linux 3 channel.

The unique Digital Certificate for the system is generated on the system in `/etc/sysconfig/rhn/systemid`.

When using activation keys to assign channels, a couple of rules should be kept in mind:

- A key may specify either zero or one base channel. If specified, it must be a custom base channel. If not, the base channel corresponding to the system's Red Hat distribution will be chosen. For instance, you may not take a Red Hat Enterprise Linux 2.1 system and subscribe it to the Red Hat Enterprise Linux 3 channel.
- A key may specify any number of child channels. For each child channel, subscription is attempted. If the child channel matches the system's base channel, subscription succeeds. If it does not, the subscription fails silently. Refer to Section 6.6 *Channels* for more information.
- Keys may be modified by any user with the role of Activation Key Administrator or Organization Administrator (or both). These permissions are set through the **Users** tab of the RHN website. Refer to Section 6.8 *Users* — for details.
- Systems registered by activation keys are tied to the organization or overall account in which the key was created, not the key itself. After registration, a key can be safely deleted without any effect on the systems it was used to register.

# Chapter 3.

# Red Hat Network Daemon

The Red Hat Network Daemon (`rhnsd`) periodically connects to Red Hat Network to check for updates and notifications. The daemon, which runs in the background, is typically started from the initialization scripts in `/etc/init.d/rhnsd` or `/etc/rc.d/init.d/rhnsd`.

**Tip**

Provisioning-entitled systems served by an RHN Satellite Server may have actions immediately initiated or *pushed* to them. Refer to Section 6.4.2.6.1 *System Details* ⇒ *Details* for instructions on enabling this feature.

To check for updates, `rhnsd` runs an external program called `rhn_check` located in `/usr/sbin/`. This is a small application that actually makes the network connection to RHN. The Red Hat Network Daemon does not listen on any network ports or talk to the network directly. All network activity is done via the `rhn_check` utility.

## 3.1. Configuring

The Red Hat Network Daemon can be configured by editing the `/etc/sysconfig/rhn/rhnsd` configuration file. This is actually the configuration file the `rhnsd` initialization script uses. The most important setting offered by the daemon is its check-in frequency. The default interval time is four hours (240 minutes). If you modify the configuration file, you must (as root) restart the daemon with the command `service rhnsd restart` or `/etc/rc.d/init.d/rhnsd restart`.

**Important**

The minimum time interval allowed is one hour (60 minutes). If you set the interval below one hour, it will default to four hours (240 minutes).

## 3.2. Viewing Status

You can view the status of the **rhnsd** by typing the command `service rhnsd status` or `/etc/rc.d/init.d/rhnsd status` at a shell prompt.

## 3.3. Disabling

To disable the daemon, (as root) run the **ntsysv** utility and uncheck **rhnsd**. You can also (as root) execute the command `chkconfig rhnsd off`. Using these two methods will only disable the service the next time the system is started. To stop the service immediately, use the command `service rhnsd stop` or `/etc/rc.d/init.d/rhnsd stop`.

## 3.4. Troubleshooting

If you are seeing messages indicating checkins are not taking place, the RHN client on your system is not successfully reaching Red Hat Network. Make certain:

- your client is configured correctly.
- your system can communicate with RHN via SSL (port 443). You may test this by running the following command from a shell prompt:
  ```
  telnet xmlrpc.rhn.redhat.com 443
  ```
- the Red Hat Network Daemon is activated and running. You may ensure this by running the following commands:
  ```
  chkconfig --level 345 rhnsd on
  service rhnsd start
  ```
  If these are correct and your systems still indicate they are not checking in, please contact our technical support team.

# Chapter 4. Red Hat Network Alert Notification Tool

The **Red Hat Network Alert Notification Tool** is a notifier that appears on the panel and alerts users when software package updates are available for their systems. The list of updates is retrieved from the RHN Servers. The system does not have to be registered with Red Hat Network to display a list of updates; however, retrieving the updates with the **Red Hat Update Agent** requires registration with Red Hat Network and a subscription to an RHN service offering. The notifier does not send any identifiable information about the user or the system to the RHN Servers.

To use the **Red Hat Network Alert Notification Tool**, you must install the `rhn-applet` RPM package and use the X Window System.

Starting with Red Hat Enterprise Linux 3, the **Red Hat Network Alert Notification Tool** appears on the panel by default as shown in Figure 4-1.

**Figure 4-1. GNOME Panel with Red Hat Network Alert Notification Tool**

If it does not appear on the panel, you can add it:

- In Red Hat Enterprise Linux 3, select the **Main Menu Button => System Tools => Red Hat Network Alert Icon**. To ensure the icon appears on subsequent sessions, select the **Save current setup** checkbox when logging out.
- In Red Hat Enterprise Linux 2.1, select the **Main Menu Button => Panel => Add to Panel => Applet => Red Hat Network Monitor**. To move it around the panel, right-click on the applet, select **Move**, move the mouse left and right until it is in the desired location, and click the mouse to place the applet.

## 4.1. Configuring the Applet

The first time the **Red Hat Network Alert Notification Tool** is run, a configuration wizard starts. It displays the terms of service and allows the user to configure an HTTP proxy as shown in Figure 4-2.

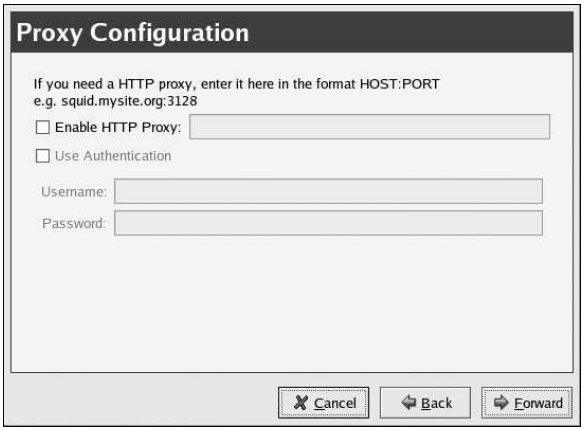


**Figure 4-2. HTTP Proxy Configuration**

If your network connection requires you to use an HTTP Proxy Server to make HTTP connections, on the **Proxy Configuration** screen, type your proxy server in the text field with the format HOST:PORT. For example, to use the proxy server http://squid.mysite.org on port 3128, enter **`squid.mysite.org:3128`** in the text field. Additionally, if your proxy server requires a username and password, select the **Use Authentication** option and enter your username and password in the respective text fields.

**Tip**

To run the configuration wizard again, right-click on the applet, and select **Configuration**.

Your preferences are written to the file `.rhn-applet.conf` in your home directory. The **Red Hat Network Alert Notification Tool** also uses the system-wide configuration file `/etc/sysconfig/rhn/rhn-applet`. Do not modify the system-wide configuration file; it is automatically generated by the application.

You can also configure the **Red Hat Network Alert Notification Tool** not to list specific packages. To configure which packages to ignore, click on the applet, and select the **Ignored Packages** tab.

## 4.2. Notification Icons

The applet displays a different icon, depending on the status of the updates. Refer to Table 4-1 for details.

| Icon | Description |
|---|---|
| | Updates are available |
| | System is up-to-date |
| | Checking for updates |
| | Error has occurred |

**Table 4-1. Red Hat Network Alert Notification Tool Icons**

If you see the icon, it is highly recommended that you apply the updates. Refer to Section 4.4 *Applying Updates* for information on applying updates.

If you have scheduled updates to be installed, you can watch the applet icon to determine when updates are applied. The icon changes to the icon after the Errata Updates are applied.

If you apply a kernel update (or the kernel update is automatically applied), the applet will display the until the system is rebooted with the new kernel. If you click on the applet, the **Available Updates** tab displays a list of packages that can be updated on your system.

## 4.3. Viewing Updates

Clicking on the **Red Hat Network Alert Notification Tool** displays a list of available updates. To alter your list of excluded packages, click the **Ignored Packages** tab and make your modifications.

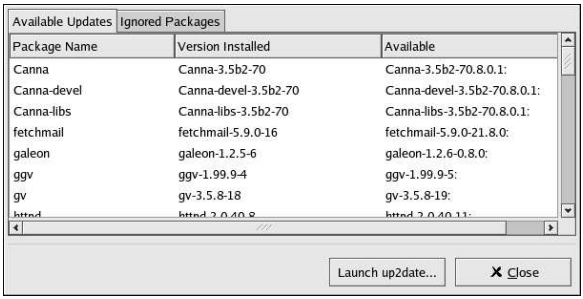


**Figure 4-3. Available Updates**

## 4.4. Applying Updates

If the system is registered with RHN and entitled to a service offering, you can apply the Errata Updates with the **Red Hat Update Agent**. To launch the **Red Hat Update Agent**, click on the applet, and then click on the **Launch up2date** button. You can also right-click on the icon and select **Launch up2date**. For more information on the **Red Hat Update Agent**, refer to Chapter 2 ***Red Hat Update Agent***.

## 4.5. Launching the RHN Website

The simplest way to obtain a comprehensive view of your system's status is to access the RHN website. This can be accomplished through the **Red Hat Network Alert Notification Tool** by right-clicking on it and selecting **RHN Website**. For more information on the RHN website, refer to Section 6.1 *Navigation*.

Chapter 5.

# Red Hat Network Registration Client

Before you begin using Red Hat Network, you need to create a username, password, and System Profile. The **Red Hat Network Registration Client** walks you through this process.

**Warning**

Only systems running Red Hat Enterprise Linux 2.1 need to use this separate **Red Hat Network Registration Client** before starting the **Red Hat Update Agent**. Systems running Red Hat Enterprise Linux 3 have this registration functionality built into the **Red Hat Update Agent**. After registering your system, refer to Chapter 2 ***Red Hat Update Agent*** for instructions on starting the **Red Hat Update Agent** and begin steps listed in Section 2.3 *Setup and Use*.

## 5.1. Configuring the Red Hat Network Registration Client

To start the graphical interface for configuring the application to connect through an HTTP proxy server, type the following command at a shell prompt:

```
rhn_register --configure
```

The window shown in Figure 5-1 will appear.

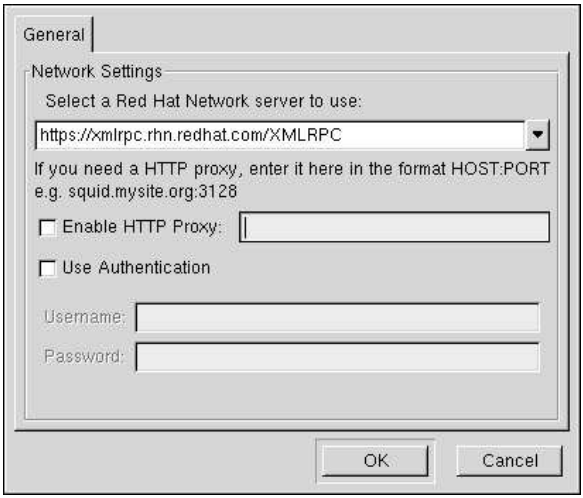


**Figure 5-1. Red Hat Network Registration Client Configuration**

To start the command line version, use the command:

```
rhn_register --nox --configure
```

It has more configuration options than the graphical version.

You will be presented with a list of options and their current values:

```
0.  enableProxyAuth    No
1.  noSSLServerURL     http://xmlrpc.rhn.redhat.com/XMLRPC
2.  oemInfoFile        /etc/sysconfig/rhn/oeminfo
3.  enableProxy        No
4.  networkSetup       Yes
5.  httpProxy
6.  proxyUser
7.  serverURL          https://xmlrpc.rhn.redhat.com/XMLRPC
8.  proxyPassword
9.  debug              No

Enter number of item to edit <return to exit, q to quit without saving>:
```

Enter the number of the item that you want to modify, and enter a new value for the option. When you finish changing your configuration, press [Enter] to save your changes and exit. Press [q] and then [Enter] to quit without saving your changes.

The most common options configured are `enableProxy` and `httpProxy` to enable a proxy server. To enable a proxy server, change the value for `enableProxy` to **`Yes`** and the value of `httpProxy` to the name of the proxy server and port number in the format http://HOST:PORT. For example, to use the proxy server http://squid.mysite.org on port 3128, you would change the value to **`http://squid.mysite.org:3128`**.

If you require a proxy username and password, set `enableProxyAuth` to **`Yes`** to enable username/password authentication for the proxy, and set `proxyUser` and `proxyPassword` to the appropriate username and password for the proxy.

To bypass SSL, in `/etc/sysconfig/rhn/rhn_register` change the protocol for `serverURL` from **`https`** to **`http`**.

## 5.2. Starting the Red Hat Network Registration Client

You must be root to register a system with RHN. If you start the **Red Hat Network Registration Client** as a standard user, you will be prompted to enter the root password before proceeding.

**Important**

If your username is part of a larger organizational account, you should take caution when registering your systems. By default, all systems registered with the **Red Hat Network Registration Client** end up in the Ungrouped section of systems visible only to Organization Administrators. To ensure you retain management of these systems, Red Hat recommends your organization create an activation key associated with a specific system group and grant you permissions to that group. You may then register your systems using that activation key and find those System Profiles within RHN immediately. Refer to Section 2.5 *Registering with Activation Keys* for instructions.

To start the **Red Hat Network Registration Client**, use one of the following methods:

1. On the GNOME desktop, go to the **Main Menu Button** (on the Panel) => **Programs** => **System** => **Red Hat Network**
2. On the KDE desktop, go to the **Main Menu Button** (on the Panel) => **System** => **Red Hat Network**

3. Type the command `rhn_register` at a shell prompt (for example an **XTerm** or **GNOME terminal**)
4. If you are not running the X Window System, type the command `rhn_register` at a virtual console or remote terminal. Refer to Section 5.7 *Text Mode RHN Registration Client* for further details.

**Caution**

You must use **Python 1.5.2-24** or later with Secure Sockets Layer (SSL) support. If not, the information you transfer will not be encrypted. If you have an earlier version of Python, you will see the message shown in Figure 5-2. To determine the version of Python on your system, use the command `rpm -q python`. It is strongly recommended you use **Python 1.5.2-24** or later.

Your system libraries do not support SSL (secure) connections. Any data that you send or receive from redhat.com will be transmitted in the clear. Continue anyway?
Yes
No

**Figure 5-2. Use Python 1.5.2-24 or later**

If you have already registered your system and try to register it again, the dialog box shown in Figure 5-3 will appear. If you continue, it will overwrite your existing Digital Certificate file (`/etc/sysconfig/rhn/systemid`), and you will create a different System Profile. You will no longer be able to use your previous System Profile — be sure this is what you want to do before you choose **Yes**.

If you overwrite an existing system registration, you can delete the unused profile via the website at https://rhn.redhat.com.

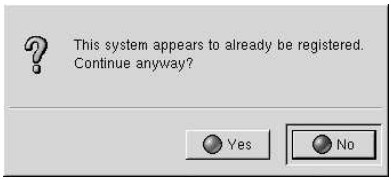


**Figure 5-3. Warning: This System Already Registered**

The opening screen for the **Red Hat Network Registration Client** gives you a brief overview of the services available and the steps required to register (see Figure 5-4). Click **Next** to continue with the registration process. If you click **Cancel**, the registration process will end and no information will be sent.

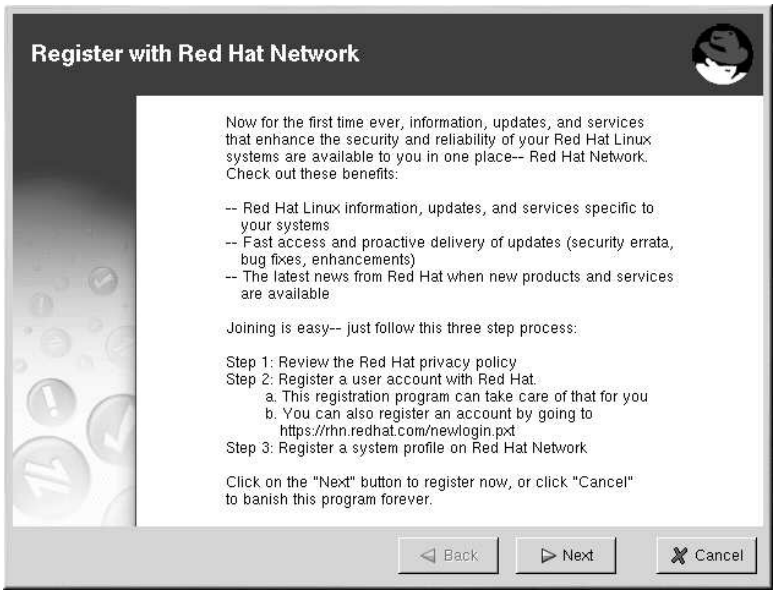
Register with Red Hat Network
Now for the first time ever, information, updates, and services that enhance the security and reliability of your Red Hat Linux systems are available to you in one place-- Red Hat Network. Check out these benefits:
-- Red Hat Linux information, updates, and services specific to your systems
-- Fast access and proactive delivery of updates (security errata, bug fixes, enhancements)
-- The latest news from Red Hat when new products and services are available
Joining is easy-- just follow this three step process:
Step 1: Review the Red Hat privacy policy
Step 2: Register a user account with Red Hat.
a. This registration program can take care of that for you
b. You can also register an account by going to https://rhn.redhat.com/newlogin.pxt
Step 3: Register a system profile on Red Hat Network
Click on the "Next" button to register now, or click "Cancel" to banish this program forever.
Back
Next
Cancel

**Figure 5-4. Welcome Screen**

Red Hat is committed to protecting your privacy (see Figure 5-5). The information gathered during the Red Hat Network registration process is used to create a System Profile. The System Profile is essential if you wish to receive update notifications about your system.

Step 1: Review the Red Hat Privacy Statement
Privacy Statement
When it comes to your privacy, our promise is simple. Your personal information is yours, not ours. In fact, we feel so strongly about it that we encourage you to read our complete privacy policy below, so that you are comfortable with how any information you provide may be used.
We think our customers understand better than anyone else how Red Hat can most effectively serve their needs. Because of this, Red Hat makes every effort to allow our customers to define the relationship they will have with us. We ask our customers how they would like Red Hat to communicate with them, if at all. We disclose how we will be using our customers' information through documents like this one, or by answering individual questions customers may ask. Also, we never sell our customers' information or provide it to others without making it clear that we intend to do so at the time the information is collected.
If you have any questions about any of these practices, please feel free to contact us at feedback@redhat.com.
Information Collected During Web Registration
Back
Next
Cancel

**Figure 5-5. Red Hat Privacy Statement**

## 5.3. Registering a User Account

Before you can create a System Profile, you must create a user account. The only required information in this section is a unique username, password, and a valid email address.

In the screen shown in Figure 5-7, you must choose a username and password. Once logged in to Red Hat Network, you can modify your preferences, view your existing System Profile, or obtain the latest Red Hat software packages. You must choose a unique username. If you enter one already in use, you will see an error message (see Figure 5-6). Try different usernames until you find one that has not been used.

**Figure 5-6. Error: Username Already Exists**

**Note**

If you are already a member of redhat.com, you can use the same user name and password. However, you will still need to continue with the registration process to create your System Profile.

Your username has the following restrictions:

- Cannot contain any spaces
- Cannot contain the characters &, +, %, or '
- Is not case-sensitive, thereby eliminating the possibility of duplicate usernames differing only by capitalization

In addition, the following restrictions apply to both your username and password:

- Must be at least four characters long
- Cannot contain any tabs
- Cannot contain any line feeds

Passwords are case-sensitive for obvious reasons.

If you have already registered a machine and created a System Profile, you can add a new machine to your account. Run the **Red Hat Network Registration Client** on the new machine you wish to add, and enter your existing Red Hat Network username and password. The new machine will be added to your existing account, and you can log into Red Hat Network with your username and password to view all your systems simultaneously.

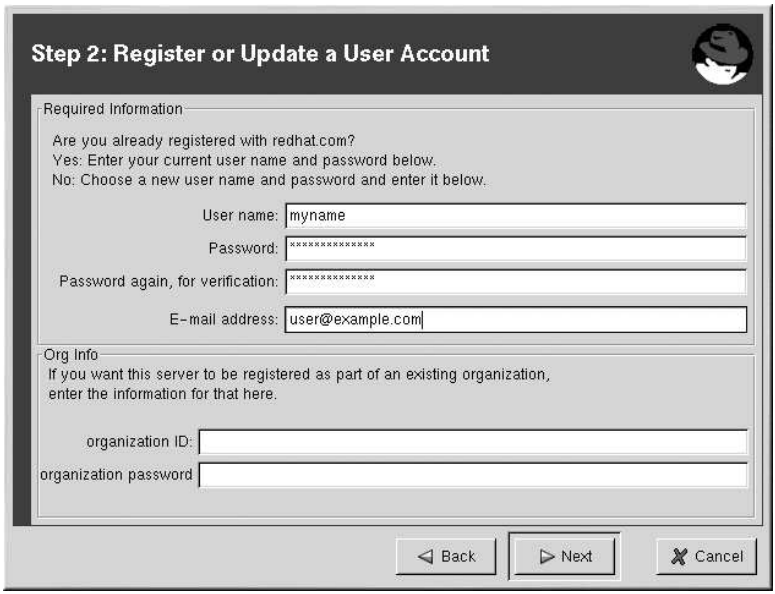
Step 2: Register or Update a User Account
Required Information
Are you already registered with redhat.com?
Yes: Enter your current user name and password below.
No: Choose a new user name and password and enter it below.
User name:
myname
Password:
Password again, for verification:
E-mail address:
user@example.com
Org Info
If you want this server to be registered as part of an existing organization,
enter the information for that here.
organization ID:
organization password
Back
Next
Cancel

**Figure 5-7. Create a Unique Username and Password**

Most users can leave the **Org Info** section blank. If you have an existing organization account, work with your Organization Administrator to ensure your system is added to that account. This will require entering your organization's ID and password in the provided text fields. If the values are valid, the system will be added to the organization's Red Hat Network account. Your Organization Administrator can then create your user account through the **Users** category of the RHN website. Refer to Section 6.8.2.1 *Create User* — for instructions.

Click **Next** to continue.

## 5.4. Registering a System Profile

Now that you have a user account, you can create a System Profile that consists of hardware and software information about your Red Hat Linux system. The software System Profile information is used by Red Hat Network to determine what software update notifications you receive.

### 5.4.1. Hardware System Profile

After creating a username and password for your Red Hat Network account, the **Red Hat Network Registration Client** probes your system for the following information:

- Red Hat Linux version
- Hostname
- IP address
- CPU model
- CPU speed
- Amount of RAM
- PCI devices
- Disk sizes
- Mount points

The next step is choosing a profile name for your system as shown in Figure 5-8. The default value is the hostname for the system. You may modify this to be a more descriptive string, such as **`Email Server for Support Team`**, if you find it more helpful. Optionally, you can enter a computer serial or identification number for the system.

If you do not wish to include information about your hardware or network in your System Profile, deselect **Include information about hardware and network** (see Figure 5-8).

Click **Next** to continue with the registration process.

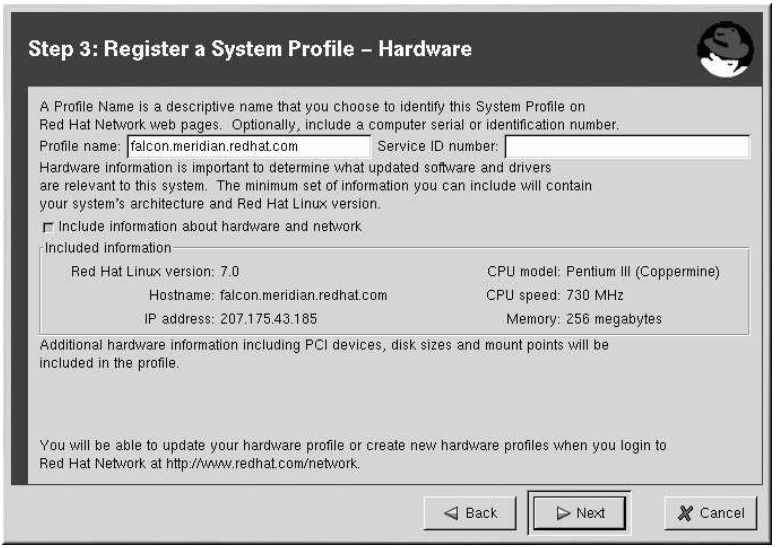
Step 3: Register a System Profile – Hardware
A Profile Name is a descriptive name that you choose to identify this System Profile on Red Hat Network web pages. Optionally, include a computer serial or identification number.
Profile name: falcon.meridian.redhat.com
Service ID number:
Hardware information is important to determine what updated software and drivers are relevant to this system. The minimum set of information you can include will contain your system's architecture and Red Hat Linux version.
Include information about hardware and network
Included information
Red Hat Linux version: 7.0
CPU model: Pentium III (Coppermine)
Hostname: falcon.meridian.redhat.com
CPU speed: 730 MHz
IP address: 207.175.43.185
Memory: 256 megabytes
Additional hardware information including PCI devices, disk sizes and mount points will be included in the profile.
You will be able to update your hardware profile or create new hardware profiles when you login to Red Hat Network at http://www.redhat.com/network.
Back
Next
Cancel

**Figure 5-8. System Profile - Hardware**

## 5.4.2. Software System Profile

The software System Profile consists of a list of RPM packages for which you wish to receive notifications. The **Red Hat Network Registration Client** shows you a list of all RPM packages listed in the RPM database on your system and then allows you to customize the list by deselecting packages.

### 5.4.2.1. Gathering RPM Database Information

Only those packages you choose during this part of the registration will be included in your System Profile, and you will only receive notifications about the packages in your System Profile. Thus, if you use an older version of a package and deselect it from the list, it will not be replaced with a newer version. This RPM list can be modified through the Red Hat Network website or by using the **Red Hat Update Agent**. Figure 5-9 shows the progress bar you will see while the **Red Hat Network Registration Client** gathers a list of the RPM packages installed on your system. This operation may take some time depending on your system.

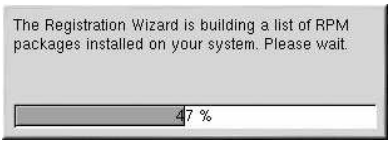


**Figure 5-9. Registration Wizard**

Once the RPM package list is built, the list will be displayed as shown in Figure 5-10. Deselecting **Include RPM Packages installed on this system in my System Profile** will omit this information from your System Profile.

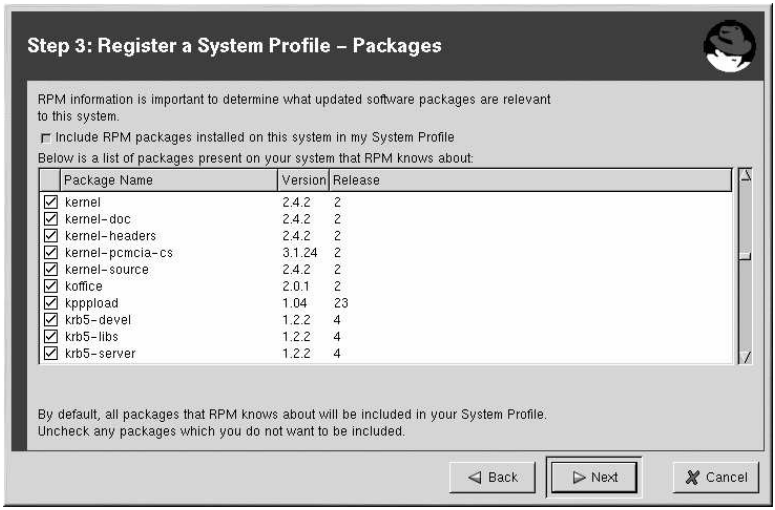
Step 3: Register a System Profile – Packages
RPM information is important to determine what updated software packages are relevant to this system.
Include RPM packages installed on this system in my System Profile
Below is a list of packages present on your system that RPM knows about:
Package Name
Version
Release
kernel 2.4.2 2
kernel-doc 2.4.2 2
kernel-headers 2.4.2 2
kernel-pcmcia-cs 3.1.24 2
kernel-source 2.4.2 2
koffice 2.0.1 2
kpppload 1.04 23
krb5-devel 1.2.2 4
krb5-libs 1.2.2 4
krb5-server 1.2.2 4
By default, all packages that RPM knows about will be included in your System Profile.
Uncheck any packages which you do not want to be included.
Back
Next
Cancel

**Figure 5-10. RPM Package Information**

### 5.4.2.2. Choosing RPM Packages to Exclude from the System Profile

By default, all RPM packages in your RPM database are included in your System Profile to be updated by Red Hat Network. To exclude a package, uncheck the package from the list by clicking the checkbox beside the package name. For example, Figure 5-11 shows that the **procmail**, **procps**, and **psgml** packages have been omitted from the package list.

Choose which packages to exclude, if any, from the System Profile, and click **Next** to continue with the registration process.

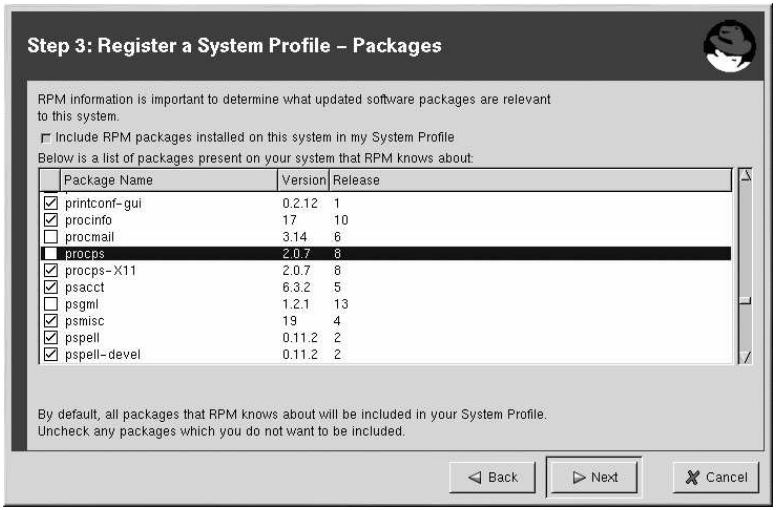
Step 3: Register a System Profile – Packages
RPM information is important to determine what updated software packages are relevant to this system.
Include RPM packages installed on this system in my System Profile
Below is a list of packages present on your system that RPM knows about:
Package Name
Version
Release
printconf-gui 0.2.12 1
procinfo 17 10
procmail 3.14 6
procps 2.0.7 8
procps-X11 2.0.7 8
psacct 6.3.2 5
psgml 1.2.1 13
psmisc 19 4
pspell 0.11.2 2
pspell-devel 0.11.2 2
By default, all packages that RPM knows about will be included in your System Profile.
Uncheck any packages which you do not want to be included.
Back
Next
Cancel

**Figure 5-11. Choose which RPM Packages to Exclude from System Profile**

## 5.5. Finishing Registration

As seen in Figure 5-12, the last step of registration is to confirm that you want to send your System Profile to the Red Hat Network. If you choose **Cancel** at this point, no information will be sent. Clicking **Next** will submit your RHN System Profile.

Send Profile Information to Red Hat Network
We are finished collecting information for the System Profile.
Click "Next" to send this System Profile to Red Hat Network. Click "Cancel" and no information will be sent. You can run the registration program later by typing rhn_register at the command line.
Back
Next
Cancel

**Figure 5-12. Finished Collecting Information for System Profile**

Figure 5-13 shows the progress bar you will see while your profile is being sent. This process may take some time depending on your connection speed.

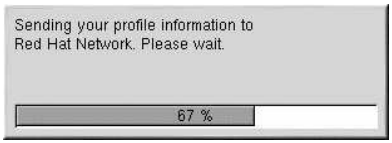


**Figure 5-13. Send System Profile to Red Hat Network**

You will know your System Profile has been successfully sent when you see the **Registration Finished** screen (Figure 5-14). Click **Finish** to exit the **Red Hat Network Registration Client**.

After completing the registration, you must entitle your system to an RHN service level. Refer to Section 5.6 *Entitling Your System* for details.

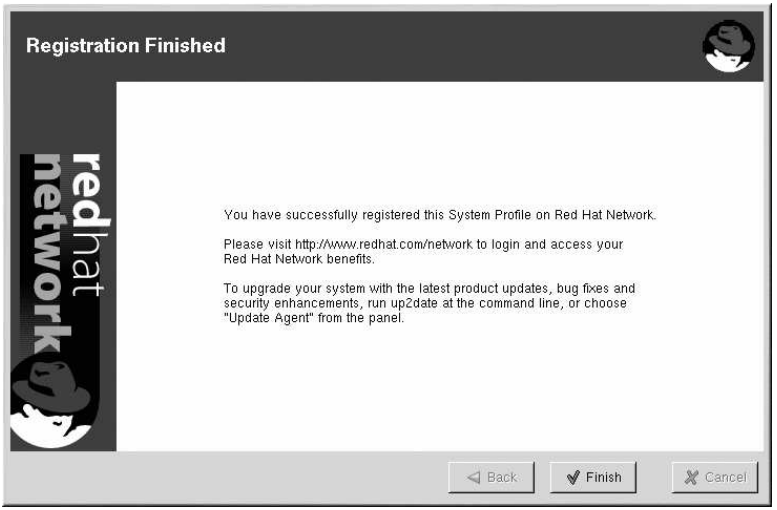
Registration Finished
redhat network
You have successfully registered this System Profile on Red Hat Network.
Please visit http://www.redhat.com/network to login and access your Red Hat Network benefits.
To upgrade your system with the latest product updates, bug fixes and security enhancements, run up2date at the command line, or choose "Update Agent" from the panel.
Back
Finish
Cancel

**Figure 5-14. Registration Finished**

## 5.6. Entitling Your System

Now that you have registered your system, it must be entitled before you can receive updated packages. In other words, you must subscribe it to a service level offering. Everyone automatically receives one free Demo entitlement after creating an account by registering a system for RHN or creating a redhat.com account.

To entitle a system, go to http://rhn.redhat.com and log in using the same username and password you just used in the **Red Hat Network Registration Client**. Click **Systems** on the top navigation bar and then **Systems Entitlements** in the left navigation bar. The **System Entitlements** page displays the number of available entitlements, or subscriptions, at the bottom.

If you have one or more subscriptions left, make a selection from the dropdown menu under the **Entitlement** column beside the name of the system you just registered. Only increases in entitlement levels are allowed. Systems cannot be re-entitled to a lower entitlement level. For instance, a system entitled to the Update service level can be promoted to the Management level, but this action cannot be reversed. Then click the **Update Entitlements** button at the bottom of the page.

**Warning**

Changing a system's entitlement is an irreversible action. You may be unable to change the entitlement levels of some systems. For more information, refer to the RHN entitlement policy linked from the **System Entitlements** page.

The number of entitlements remaining decreases, and your system becomes ready to use the **Red Hat Update Agent** and RHN website. Refer to Chapter 2 ***Red Hat Update Agent*** and Chapter 6 *Red Hat Network Website* for details on how to use them. If you do not have any entitlements left, click the **Buy more system entitlements now** link at the top of the **System Entitlements** page to make additional purchases.

## 5.7. Text Mode RHN Registration Client

If you are not running the X Window System, the **Red Hat Network Registration Client** starts in text mode.

You can force the **Red Hat Network Registration Client** to run in text mode with the command:

```
rhn_register --nox
```

The screens for the text mode **Red Hat Network Registration Client** are almost identical to the screens for the graphical **Red Hat Network Registration Client**. Some of the text in the text mode version is more concise due to lack of space in the interface. However, there is an equal number of screens and fields in both versions. Thus, if you are using the text mode version, you can still follow the instructions that begin in Section 5.2 *Starting the **Red Hat Network Registration Client***.

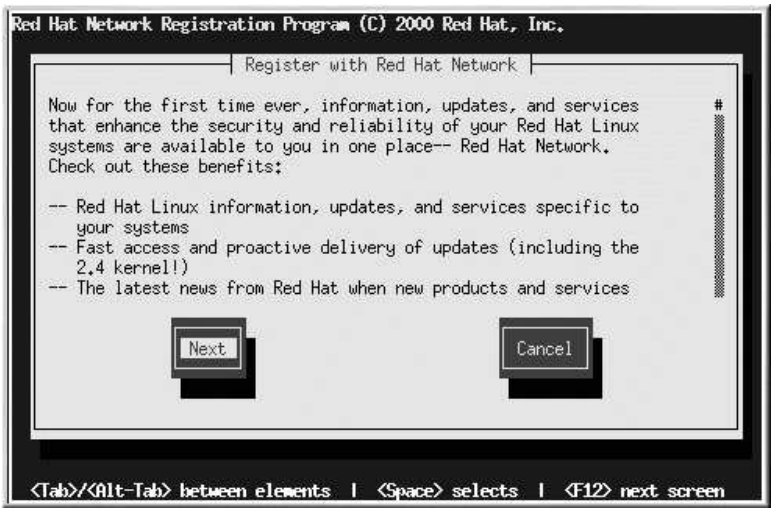
Red Hat Network Registration Program (C) 2000 Red Hat, Inc.
Register with Red Hat Network
Now for the first time ever, information, updates, and services that enhance the security and reliability of your Red Hat Linux systems are available to you in one place-- Red Hat Network. Check out these benefits:
-- Red Hat Linux information, updates, and services specific to your systems
-- Fast access and proactive delivery of updates (including the 2.4 kernel!)
-- The latest news from Red Hat when new products and services
Next
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

**Figure 5-15. Text Mode Welcome Screen**

redhat

Chapter 6.

# Red Hat Network Website

You can use the Red Hat Network website to manage multiple Red Hat Enterprise Linux systems simultaneously, including viewing Errata Alerts, applying Errata Updates, and installing packages. This chapter seeks to identify all of categories, pages, and tabs within the website and explain how to use them.

## 6.1. Navigation

The *top navigation bar* is divided into tabs of primary *categories* containing *pages* linked from the *left navigation bar*.

### 6.1.1. Entitlement Views

Keep in mind, since this guide covers all entitlement levels, some tabs, pages, and even whole categories described here may not be visible to you. For this reason, icons are used here to identify which functions are available to each entitlement level.

| Icon | Entitlement |
|---|---|
| | Management or higher |
| | Provisioning |
| | Monitoring |

**Table 6-1. Entitlement Icons**

If no icon follows a category, page, or tab label within this chapter, the area described is available to all Red Hat Network users. If an icon does follow, the associated entitlement is needed. Remember that Provisioning inherits all of the functions of Management.

If an icon precedes a paragraph, only the specific portion of the page or tab discussed afterward required the indicated entitlement level. When a page or tab is associated with a particular entitlement level, all of its tabs and subtabs require at least the same entitlement level but may need a higher entitlement. Regardless, each tab is identified separately.

### 6.1.2. Categories and Pages

This section summarizes all of the categories and primary pages (those linked from the top and left navigation bars) within the RHN website. It does not list the many subpages, tabs and subtabs accessible from the left navigation bar and individual pages. Each area of the website is explained in detail later in this chapter:

- **Your RHN** — View and manage your primary account information and obtain help.
  - **Your RHN** — Obtain a quick overview of your account. It notifies you if your systems need attention, provides a quick link to go directly to them, and displays the most recent Errata Alerts for your account.
  - **Your Account** — Update your personal profile and addresses.

- **Your Preferences** — Indicate if you wish to receive email notifications about Errata Alerts for your systems, set how many items are displayed at one time for lists such as system lists and system group lists, set your time zone, and identify your contact options.
- **Purchase History** — View a history of your entitlements, including the expiration date and the number available.
- **Help** — Learn how to use Red Hat Network and receive support if needed.

- **Systems** — Manage your systems here.
  - **Overview** —  — View a summary of your systems or system groups showing how many Errata Alerts each system has and which systems are entitled.
  - **Systems** — Select and view subsets of your systems by specific criteria, such as Out of Date, Unentitled, Ungrouped, and Inactive.
  - **System Groups** —  — List your system groups. Create additional groups.
  - **System Set Manager** —  — Perform actions on currently selected systems.
  - **System Entitlements** — Change the entitlement levels of systems.
  - **Advanced Search** —  — Quickly search all of your systems by specific criteria, such as name, hardware, devices, system info, networking, packages, and location.
  - **Activation Keys** —  — Generate an activation key for an RHN-entitled system. This activation key can be used to grant a specified level of entitlement or group membership to a newly registered system with the `rhnreg_ks` command.
  - **Stored Profiles** —  — View system profiles used to provision systems.
  - **Custom System Info** —  — Create and edit system information keys containing completely customizable values that can be assigned while provisioning systems.
  - **Kickstart** —  — Display and modify various aspects of kickstart profiles used in provisioning systems.

- **Errata** — View and manage Errata Alerts here.
  - **Errata** — List Errata Alerts and download associated RPMs.
  - **Advanced Search** — Search Errata Alerts based on specific criteria, such as synopsis, advisory type, and package name.
- **Channels** — View and manage the available RHN channels and the files they contain.
  - **Software Channels** — View a list of all software channels and those applicable to your systems.
  - **Channel Entitlements** — View a list of software channels for which you have paid, as well as the systems associated with each.
  - **Easy ISOs** — Access priority downloading of Red Hat ISO images. ISO images are used to write to CD.
  - **Package Search** — Search packages using all or some portion of the package name.
  - **Manage Config Channels** —  — Create and edit channels used to deploy configuration files.

- **Schedule** — Keep track of your scheduled actions.

- **Pending Actions** — List scheduled actions that have not been completed.
- **Failed Actions** — List scheduled actions that have failed.
- **Completed Actions** — List scheduled actions that have been completed. Completed actions can be archived at any time.
- **Archived Actions** — List completed actions that have been selected to archive.

- **Users** — — View and manage users for your organization.
  - **User List** — — List users for your organization.
- **Monitoring** — — Run probes and receive notifications regarding systems.
  - **Probe Status** — — View probes by state.
  - **Notification** — — View contact methods established for yor organization.
  - **Scout Config Push** — — Reconfigure your monitoring infrastructure.
  - **Global Config** — — Change organization-wide monitoring settings.

### 6.1.3. Errata Alert Icons

Throughout Red Hat Network you will see three Errata Alert icons. represents a Security Alert. represents a Bug Fix Alert. represents an Enhancement Alert.

In the **Your RHN** page, click on the Errata advisory to view details about the Erratum or click on the number of affected systems to see which are affected by the Errata Alert. Both links take you to tabs of the **Errata Details** page. Refer to Section 6.5.2.2 *Errata Details* for more information.

### 6.1.4. Quick Search

In addition to the Advanced Search functionality offered within some categories, the RHN website also offers a Quick Search tool near the top of each page. To use it, select the item type (such as packages) and type a keyword that will be used to look for a name match. Then click the **Search** button. Your results will appear at the bottom of the page. Refer to the appropriate category for instructions on using these results.

### 6.1.5. Systems Selected

Also near the top of the page is a tool for keeping track of the systems you've selected for use in the System Set Manager. It identifies the number selected at all times and provides the means to work with them. Clicking the **Clear** button deselects all systems, while clicking the **Manage** button launches the System Set Manager with your selected systems in place.

These systems can be selected in a number of ways. Only systems entitled to the Management and Provisioning service are eligible for selection. On all system and system group lists, a Select column exists for this purpose. Select the checkboxes next to the systems or groups and click the **Update List** button below the column. Each time, the Systems Selected tool at the top of the page will change to reflect the new number of systems ready for use in the System Set Manager. Refer to Section 6.4.4 *System Set Manager* — for details.

### 6.1.6. Lists

The information within most categories is presented as lists. These lists have some common features for navigation. For instance, you can navigate through virtually all lists by clicking the back and next arrows above and below the right side of the table. Some lists also offer the ability to retrieve items alphabetically by clicking the letters above the table.

## 6.2. Logging into the RHN Website

In a Web browser, go to http://rhn.redhat.com. The page shown in Figure 6-1 will be displayed.

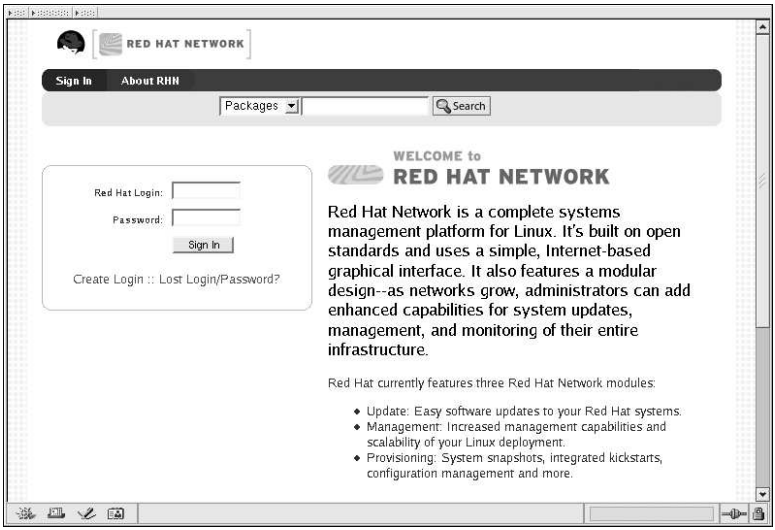
RED HAT NETWORK
Sign In
About RHN
Packages
Search
Red Hat Login:
Password:
Sign In
Create Login :: Lost Login/Password?
WELCOME to
RED HAT NETWORK
Red Hat Network is a complete systems management platform for Linux. It's built on open standards and uses a simple, Internet-based graphical interface. It also features a modular design--as networks grow, administrators can add enhanced capabilities for system updates, management, and monitoring of their entire infrastructure.
Red Hat currently features three Red Hat Network modules:
Update: Easy software updates to your Red Hat systems.
Management: Increased management capabilities and scalability of your Linux deployment.
Provisioning: System snapshots, integrated kickstarts, configuration management and more.

**Figure 6-1. RHN Website**

If you have not registered a system yet or do not have a redhat.com account, create a new account by clicking **Create Account**. After creating a new user account, you must register your system before using RHN. Refer to Chapter 2 ***Red Hat Update Agent*** for step-by-step instructions.

After registering your system with Red Hat Network, go back to http://rhn.redhat.com and complete the username and password fields with the same information established during registration. Click the **Sign In** link near the top to display the fields, if they are not already visible. Once complete, click the **Sign In** button.

## 6.3. Your RHN

After logging into the website of Red Hat Network, the first page to appear is **Your RHN**. This page contains important information about your systems, including summaries of system status, actions, and Errata Alerts.

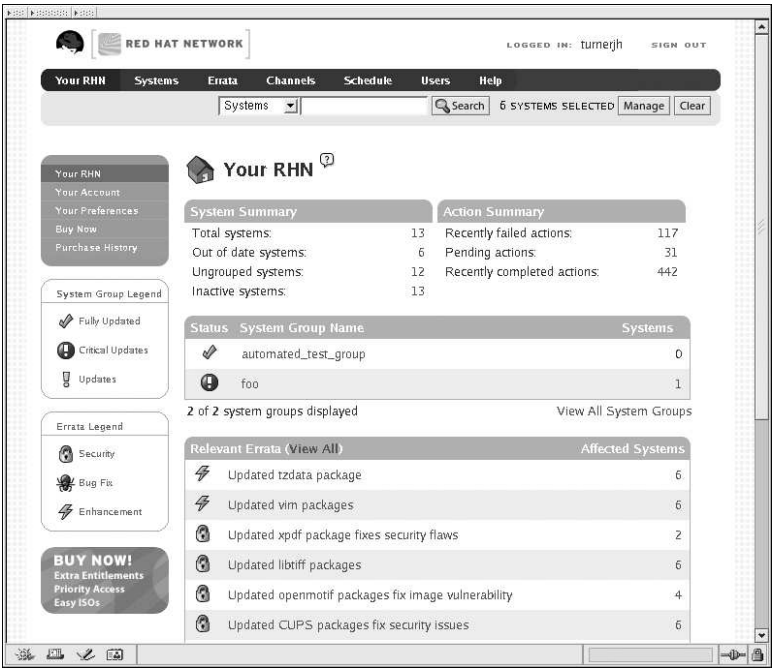


**Figure 6-2. Your Red Hat Network**

The top of the page shows how many systems need attention, provides a link to quickly view those systems, and displays a summary of scheduled actions. Refer to Section 6.4.2 *Systems* for information on using the **Systems** pages.

The **System Summary** section of **Your RHN** page provides the following information:

- **Total Systems** — Number of total systems that you have registered for your organization.
- **Out of Date Systems** — Number of registered systems that have applicable Errata Alerts that have not been applied.
- **Unentitled Systems** — Number of systems that are not entitled.
- **Ungrouped Systems** — Each system may be a member of one or more groups. The number of ungrouped systems refers to systems that are not yet members of any system group.
- **Inactive Systems** — Number of systems that have not checked into RHN for 24 hours or more. Refer to Section 6.4.2.5 *Inactive* for details.

The **Action Summary** section provides the following information about events scheduled in the past week:

- **Recently Failed Actions** — Number of scheduled actions that did not succeed.
- **Pending Actions** — Number of scheduled actions that have not yet been completed.
- **Recently Completed Actions** — Number of scheduled actions that succeeded.

The **System Groups** section gives you access to the groups of systems you establish. Clicking on the links in this section takes you to the **System Group Details** pages. Refer to Section 6.4.3.3 *System Group Details* — for more information.

The **Errata** section lists all and relevant Errata Alerts. You may toggle between All and Relevant by clicking the **View All** or **View Relevant** link at the top of the table. This view is retained until you toggle it by again clicking the link.

Relevant Errata are those derived from software channels to which your systems are subscribed. They refer to versions of packages that are newer than those installed on the systems. To go to a complete list of applicable Errata Alerts for your systems stored in the **Errata** category, click **View All Relevant Errata** in the bottom right-hand corner.

You can return to this page by clicking **Your RHN** on the left navigation bar.

## 6.3.1. Your Account

The **Your Account** page allows you to modify your personal information, such as name, password, and title. To modify any of this information, merely make the changes in the appropriate text fields and click the **Update** button in the bottom right-hand corner.

Remember, if you change your Red Hat Network password (the one used to log into RHN and redhat.com), you will not see your new one as you type it for security reasons. Also for security, your password is represented by 12 asterisks no matter how many characters it actually contains. Replace the asterisks in the **Password** and **Password Confirmation** text fields with your new password.

### 6.3.1.1. Addresses

The **Addresses** page allows you to manage your mailing, billing and shipping addresses, as well as the associated phone numbers. Just click **Edit this address** below the address to be modified, make the changes, and click **Update Address**.

### 6.3.1.2. Change Email

The email address listed in the **Your Account** page is the address Red Hat Network sends email notifications to, if you select to receive Errata Alerts or daily summaries for your systems on the **Your Preferences** page.

To change your preferred email address, click **Change Email** in the left navigation bar. You will then be asked for the new email address. Enter it and click the **Update** button. A confirmation email will be sent to the new email address; responding to the confirmation email will validate the new email address. Note that false email addresses such as those ending in "@localhost" are filtered and rejected.

### 6.3.1.3. Account Deactivation

The **Account Deactivation** page provides a means to cancel your Red Hat Network service. It presents steps for manual deactivation or instructions for contacting Customer Service, depending on your level of service. Deactivation of the account should occur within one business week.

### 6.3.2. Your Preferences

The **Your Preferences** page allows you to configure Red Hat Network options, including:

- Email Notifications — Determine whether you want to receive email every time an Errata Alert is applicable to one or more systems in your RHN account.

**Important**

This setting also enables Management and Provisioning customers to receive a daily summary of system events. These include actions affecting packages, such as scheduled Errata Updates, and system reboots or failures to check in. In addition to selecting this checkbox, you must identify each system to be included in this summary email. (By default, all Management and Provisioning systems are included in the summary.) This can be done either through the **System Details** page individually or through the **System Set Manager** interface for multiple systems at once. Note that RHN will send these summaries only to verified email addresses. To disable all messages, simply deselect this checkbox.

- RHN List Page Size — Maximum number of items that will appear in a list on a single page. If more items are in the list, clicking the **Next** button will display the next group of items. This preference applies to system lists, Errata lists, package lists, and so on.
- Time Zone — Set your time zone so that scheduled actions are scheduled according to the time in your time zone.
- Red Hat Contact Options — Identify what ways (email, phone, fax, or mail) Red Hat may contact you.

After making changes to any of these options, click the **Save Preferences** button on the bottom right-hand corner.

### 6.3.3. Purchase History

The **Purchase History** page displays a list of your RHN purchases, including the dates bought and expired and the number purchased.

### 6.3.4. Help

The **Help** pages provide access to the full suite of documentation and support available to RHN users. Click **Help** in the **Your RHN** category to see a list of options available to you.

#### 6.3.4.1. Help Desk

The **Help Desk** page summarizes the help options available within this section. Click either the links within this page or the buttons on the left navigation bar to explore further.

#### 6.3.4.2. Quick Start Guide

The **Quick Start Guide** page contains a brief overview of Red Hat Network and its many features. If you are unfamiliar with RHN, it is recommended you read this guide in its entirety. Topics covered include registering your systems, applying Errata Updates, using one-click updates, and troubleshooting.

#### 6.3.4.3. FAQ

The **FAQ** page lists Frequently Asked Questions and answers to those questions. These are broken down into the following categories, each represented by a separate button and page: Top Ten, General, Account Management, Getting Started, Service Levels, Using RHN, Technical Questions, Management Service, Privacy/Legal, Policies, Definitions, and All.

#### 6.3.4.4. Reference Guide

The **Reference Guide** page takes you to this same document, the most comprehensive set of instructions for using Red Hat Network. Note that links to other technical guides may also appear in the left navigation bar, depending on the entitlement level and product offering of the account with which you logged in.

#### 6.3.4.5. Contact RHN

The **Contact RHN** page provides methods by which customers may obtain help. Specifically, logged out users have access to the FAQ, Customer Service email address, and rhn-users mailing list. Logged in Demo customers have access to the above, as well as an online form that can be submitted to rhn-feedback or the Customer Service address. Logged in paid users have access to all of the above. In addition, the online form enables them to submit requests for technical support.

The Customer Service address handles billing and purchasing questions, while the rhn-users list enables customers to help one another. The rhn-feedback address collects customer input and provides an auto response, but nothing more. The technical support form ensures the customer will get a personalized and helpful response in a timely manner.

#### 6.3.4.6. Terms & Conditions

The **Terms & Conditions** page displays the RHN Network Services Use and Subscription Agreement.

#### 6.3.4.7. Outage Policy

The **Outage Policy** page identifies scheduled maintenance windows for Red Hat Network and provides the means to subscribe to the Email Outage List (rhn-outage-list@redhat.com) to be notified of emergency and other unscheduled outages.

#### 6.3.4.8. Release Notes

The **Release Notes** page lists the notes accompanying every recent release of Red Hat Network. These notes describe all significant changes occurring in a given release cycle, from major enhancements to the user interface to minor changes to the related documentation.

#### 6.3.4.9. Get RHN Software

The **RHN Software** page provides direct links to the **Red Hat Update Agent** and **Red Hat Network Registration Client** for every supported distribution. In addition, it describes how to resolve expired Secure Sockets Layers (SSL) certificates if you are using an older version of Red Hat Enterprise Linux that shipped with a certificate that is now expired.

## 6.4. Systems

If you click the **Systems** tab on the top navigation bar, the **Systems** category and links appear. The pages in the **Systems** category allow you to select systems so that you can perform actions on them and create System Profiles.

### 6.4.1. Overview —

As shown in Figure 6-3, the **Overview** page provides a summary of your systems, including their status, number of associated Errata and packages, and entitlement level. Clicking on the name of a system takes you to its **System Details** page. Refer to Section 6.4.2.6 *System Details* for more information.

**Figure 6-3. Systems Overview**

Clicking the **View System Groups** link at the top of the **Overview** page takes you to a similar summary of your system groups. It identifies group status and displays the number of systems contained. Clicking on the number of systems takes you to the **Systems** tab of the **System Group Details** page, while clicking on the system name takes you to the **Details** tab. Refer to Section 6.4.3.3 *System Group Details* — for more information.

You can also click the **Use Group** button in the **System Groups** section of the **Overview** page to go directly to the **System Set Manager**. Refer to Section 6.4.4 *System Set Manager* — for more information.

### 6.4.2. Systems

The **Systems** page displays a list of all your registered systems. The **Systems** list contains several columns of information for each system:

- **Select** — Update-entitled systems cannot be selected. To select systems, mark the appropriate checkboxes and click the **Update List** button below the column. Selected systems are added to the **System Set Manager**. After adding systems to the **System Set Manager**, you can use it to perform actions on them simultaneously. Refer to Section 6.4.4 *System Set Manager* — for details.
- **Status** — Shows which type of Errata Alerts are applicable to the system or confirms that it is up-to-date. Some icons are linked to pages providing resolution. For instance, the standard Updates icon is linked to the **Upgrade** subtab of the packages list, while the Critical Updates icon goes directly to the **Update Confirmation** page. Also, the Not Checking In icon is linked to instructions for resolving the issue.
  - — System is up-to-date
  - — Critical Errata available, update *strongly* recommended
  - — Updates available and recommended
  - — System is locked; Actions prohibited
  - — System is being kickstarted
  - — Updates have been scheduled
  - — System not checking in properly (for 24 hours or more)
  - — System not entitled to any update service
- **Errata** — Total number of Errata Alerts applicable to the system.
- **Packages** — Total number of package updates for the system. Includes packages from Errata Alerts as well as newer packages that are not from Errata Alerts. For example, if a system is subscribed to the Red Hat Enterprise Linux 2.1 i386 channel that contains version 2.5.4 of a package because that is the version that shipped with Red Hat Enterprise Linux 2.1, but the system has version 2.5.2 of the package installed, the newer version of the package will be in the list of updated packages for the system.

**Important**

If the RHN website identifies package updates for the system, yet the **Red Hat Update Agent** responds with "Your system is fully updated" when run, a conflict likely exists in the system's package profile or in the `up2date` configuration file. To resolve the conflict, either schedule a package list update or remove the packages from the Package Exceptions list for the **Red Hat Update Agent**. Refer to Section 6.4.2.6 *System Details* or Section 2.4.1.3 *Package Exceptions Settings*, respectively, for instructions.

- **System** — The name of the system as configured when registering it. The default name is the hostname of the system. Clicking on the name of a system takes you to the **System Details** page for the system. Refer to Section 6.4.2.6 *System Details* for more information.
- **Base Channel** — The primary channel for the system, based upon its operating system distribution. Refer to Section 6.6.1 *Software Channels* for more information.
- **Entitlement** — Whether or not the system is entitled and at what service level.

Links in the left navigation bar below **Systems** enable you to select and view predefined sets of your systems. All of the options described above can be applied within these pages.

#### 6.4.2.1. All

The **All** page contains the default set of your systems. It displays every system you have permission to manage. A user has permission to manage a system if he is the only user in his organization, if he is an Organization Administrator, or if the system is a member of a group to which he has admin rights.

#### 6.4.2.2. Out of Date

The **Out of Date** page displays the systems that have applicable Errata Alerts that have not been applied.

#### 6.4.2.3. Unentitled —

The **Unentitled** page displays the systems that have not yet been entitled for Red Hat Network service.

#### 6.4.2.4. Ungrouped

The **Ungrouped** page displays the systems that have not yet been assigned to a specific system group.

#### 6.4.2.5. Inactive

The **Inactive** page displays the systems that have not checked into RHN for 24 hours or more. When the **Red Hat Update Agent** connects to RHN to see if there are any updates available or if any actions have been scheduled, this is considered a checkin. If you are seeing a message indicating checkins are not taking place, the RHN client on your system is not successfully reaching Red Hat Network for some reason. This indicates:

- The system is not entitled to any RHN service. System Profiles that remain unentitled for 180 days (6 months) are removed.
- The system is entitled, but the Red Hat Network Daemon has been disabled on the system. Refer to Chapter 3 *Red Hat Network Daemon* for instructions on restarting and troubleshooting.
- The system is behind a firewall that does not allow connections over https (port 443).
- The system is behind an HTTP proxy server that has not been properly configured.
- The system is connected to an RHN Proxy Server or RHN Satellite Server that has not been properly configured.
- The system itself has not been properly configured, perhaps pointing at the wrong RHN Server.
- The system is not on the network.
- Some other barrier exists between the system and the RHN Servers.

### 6.4.2.6. System Details

If you click on the name of a system on any page, it will display the **System Details** page for the system. From here, you may modify this information or remove the system altogether by clicking the **delete system** link on the top-right corner.

The **System Details** page is further divided into tabs:

#### *6.4.2.6.1. System Details ⇒ Details*

Displays information about the system. This is the first tab you see when you click on a system. It offers direct access to some of the functionality provided in subsequent tabs. For instance, under the System Info heading, a message should appear describing the status of this machine. If it states "Critical updates available" you may click the **update now** link to apply all relevant Errata Updates to the individual system, as you would under the **Errata** tab.

— In addition, some Management-level functions can be accessed only on this tab. Most importantly, a system may be locked by clicking the **Lock system** link near the bottom-left corner of the page. This prohibits the scheduling of any action through RHN that would affect the system, including package updates and system reboots. To undo this, click the **Unlock system** link in the same location.

— Finally, still other Provisioning-level features can be found here, as well. The most important of these is the marker indicating the client system can have actions pushed to it. This feature requires it be connected to an RHN Satellite Server that has this feature enabled and is identified by the **OSA Status** section within the **System Details** page.

Push enables Satellite customers to immediately initiate tasks on Provisioning-entitled systems, rather than wait for those systems to check in with RHN. Scheduling actions through push is identical to the process of scheduling any other action except the task will begin immediately instead of waiting the set interval.

In addition to the configuration of the Satellite, each client system to receive pushed actions must have the `osad` package installed and its service started. Refer to the *Enabling Push to Clients* section of the *RHN Satellite Server Installation Guide* for details.

The Details tab contains the following subsets of information:

##### *6.4.2.6.1.1. System Details ⇒ Details ⇒ Overview*

A summary of the system's details. In addition to the system status message, the **Overview** subtab contains basic System Info, Subscribed Channels, and System Properties. Clicking the **Alter Channel Subscriptions** link takes you to the **Channels** tab, while clicking the **Edit these properties** link takes you to the **Properties** subtab. See the following sections for more information.

##### *6.4.2.6.1.2. System Details ⇒ Details ⇒ Properties*

The profile name, entitlement level, notification choice, daily summary, auto-Errata update, and physical location of the system, including street address, city, state, country, building, room, and rack. To modify this information, make your changes and click the **Update Properties** button. Note that many of these properties can be set for multiple systems at once through the **System Set Manager** interface. Refer to Section 6.4.4 *System Set Manager* — for details. The following properties deserve additional explanation:

- **Receive Notifications of Updates/Errata** — This setting keeps you abreast of all advisories pertaining to the system. Anytime an update is produced and released for the system, a notification is sent via email.

- **Include system in daily summary report calculations** — This setting includes the system in a daily summary of system events. (By default, all Management and Provisioning systems are included in the summary.) These are actions affecting packages, such as scheduled Errata Updates, and system reboots or failures to check in. In addition to including the system here, you must choose to receive email notifications in the **Your Preferences** page of the **Your RHN** category. Refer to Section 6.3.2 *Your Preferences* for instructions. Note that RHN will send these summaries only to verified email addresses.
- **Automatic application of relevant errata** — This setting allows you have all Errata Updates automatically applied to a system. This means packages associated with Errata will be updated without any user intervention. Customers should note that Red Hat does not recommend the use of the auto-update feature for production systems because conflicts between packages and environments can cause system failures. The Red Hat Network Daemon must be enabled on the systems for this feature to work.

#### *6.4.2.6.1.3. System Details ⇒ Details ⇒ Hardware*

Detailed information about the system, including networking, BIOS, storage, and other devices. This appears only if you selected to include the hardware profile for this machine during registration. If the hardware profile looks incomplete or outdated, click the **Schedule Hardware Refresh** button to schedule a Hardware Profile update for your system. The next time the RHN Daemon connects to RHN, it will update your System Profile with the latest list of hardware.

#### *6.4.2.6.1.4. System Details ⇒ Details ⇒ Notes*

A place to create notes about the system. To add a new note, click the **create new note** button, type a subject and details, and click the **Create** button. To modify a note, click on its subject in the list of notes, make your changes, and click the **Update** button. To remove a note, click on its subject in the list of notes and then click the **delete note** button.

#### *6.4.2.6.1.5. System Details ⇒ Details ⇒ Custom Info —*

Completely customizable information about the system. Unlike a note, information included here is more formal and can be searched upon. For instance, you may decide to identify an asset tag for each system. To do this, you must first create an **`asset`** key within the **Custom System Info** page. Refer to Section 6.4.9 *Custom System Info —* for instructions. Once the key exists, you may assign a value to it by clicking **create new value** here. Click the name of the key in the resulting list and enter a value for it in the Description field, such as "Example#456." Then click the **Update Key** button.

#### *6.4.2.6.1.6. System Details ⇒ Details ⇒ Reactivation —*

A System Profile-specific activation key. This allows you to create an activation key encompassing this system's ID, history, groups, and channels. You may then use this key only once with the `rhnreg_ks` command line utility to re-register this system and regain all Red Hat Network settings. Refer to Section 2.5 *Registering with Activation Keys* for instructions. Unlike typical activation keys, which are not associated with a specific system ID, keys created here do not show up within the **Activation Keys** page.

**Warning**

When kickstarting a system with its existing RHN profile, it will use the system-specific activation key created here to reregister the system and return its other RHN settings. For this reason, you should

not regenerate, delete, or use this key (with `rhnreg_ks`) while a profile-based kickstart is in progress. If you do, the kickstart will fail.

#### *6.4.2.6.1.7. System Details ⇒ Details ⇒ Remote Command* —

The method for running a remote command on the system. To allow remote commands to be run on the client through RHN, first install the latest `rhncfg*` packages available within the RHN Provisioning child channel for the system. These may already be installed if you kickstarted the system with configuration management functionality.

Next, create the necessary directory on the target system:

```
mkdir -p /etc/sysconfig/rhn/allowed-actions/script
```

Then create a `run` file in that directory to act as a flag to RHN signaling permission to allow remote commands:

```
touch /etc/sysconfig/rhn/allowed-actions/script/run
```

You may then identify a specific user, group, and timeout period, as well as the script itself on this page. Select a date and time to begin attempting the command, and click **Schedule Remote Command**.

#### *6.4.2.6.1.8. System Details ⇒ Details ⇒ Connection*

The system's path to the package repository. This tab appears for any system in an organization that has a registered RHN Proxy Server version 3.1 or later. This subtab is designed to help you determine if updates and other information are passing through one or more RHN Proxy Servers. It identifies the Proxies being used and the order in which data passes through them to reach this system. The Proxy connecting directly to the central RHN Servers or your RHN Satellite Server is numbered '1'.

### *6.4.2.6.2. System Details ⇒ Errata*

Contains a list of Errata Alerts applicable to the system. Refer to Section 6.1.3 *Errata Alert Icons* for meanings of the icons on this tab. To apply updates, select them and click the **Apply Errata** button. Double-check the updates to be applied on the confirmation page, then click the **Confirm** button. After confirming, the action is added to the **Pending Actions** list under **Schedule**. Errata that have been scheduled cannot be selected for update. In the place of a checkbox, you will find a clock icon that, when clicked, takes you to the **Action Details** page.

To help users determine whether an update has been scheduled, a Status column exists within the Errata table. Possible values are: None, Pending, Picked Up, Completed, and Failed. This column identifies only the latest action related to an Errata. For instance, if an action fails and you reschedule it, this column will show the status of the Errata as Pending only (with no mention of the previous failure). Clicking a status other than None takes you to the **Action Details** page. This column corresponds to one on the **Affected Systems** tab of the **Errata Details** page.

### *6.4.2.6.3. System Details ⇒ Packages*

Manages the packages on the system.

— When selecting packages to install, upgrade, or remove, Provisioning customers have the option of running a remote command automatically before or after the package installation. Refer to Section 6.4.2.6.1.7 *System Details ⇒ Details ⇒ Remote Command* — for more information.

#### *6.4.2.6.3.1. System Details ⇒ Packages ⇒ Packages*

The default display of the **Packages** tab describes the options available to you and provides the means to update your package list. If after exploring the packages, you believe the list is outdated or incomplete (or you installed the packages manually and did not have RHN install them), click the **Update Package List** button on the bottom right-hand corner of this page. The next time the RHN Daemon connects to RHN, it will update your System Profile with the latest list of installed packages.

#### *6.4.2.6.3.2. System Details ⇒ Packages ⇒ List/Remove*

Lists installed packages from the system's software System Profile and enables you to remove them. Click on a package name to view its **Package Details** page. (Refer to Section 6.6.5.3 *Package Details*.) To delete packages from the system, select their checkboxes and click the **Remove Packages** button on the bottom right-hand corner of the page. A confirmation page will appear with the packages listed. Click the **Confirm** button to remove the packages.

#### *6.4.2.6.3.3. System Details ⇒ Packages ⇒ Upgrade*

Displays a list of packages that have a new version available based on the package versions in the channels for the system. Click on the latest package name to view its **Package Details** page. To upgrade packages immediately, select them and click the **Upgrade Packages** button. To download the packages as a .tar file, select them and click the **Download Packages** button. Refer to Section 6.6.5.2 *Package Download* for details.

#### *6.4.2.6.3.4. System Details ⇒ Packages ⇒ Install*

Enables you to install new packages on the system from the available channels. Click on the package name to view its **Package Details** page. To install packages, select them and click the **Install Selected Packages** button.

#### *6.4.2.6.3.5. System Details ⇒ Packages ⇒ Verify* —

Validates the packages installed on the system against its RPM database. This is the equivalent of running `rpm -V`. Specifically, this tab allows you to compare the metadata of the system's packages with information from the database, such as MD5 sum, filesize, permissions, owner, group and file size and type. To verify a package or packages, select them and click the **Verify Selected Packages** button and then confirm this action. Once finished, you can view the results by selecting this action within the **History** subtab under **Events**.

#### *6.4.2.6.3.6. System Details ⇒ Packages ⇒ Profiles* —

Gives you the ability to compare the packages on this system with the packages of stored profiles and other Management and Provisioning systems. To make the comparison with a stored profile, select that profile from the pulldown menu and click the **Compare** button. To make the comparison with another system, select it from the associated pulldown menu and click the **Compare** button. To create a stored profile based upon the existing system, click the **Create System Profile** button, enter any

additional information you desire, and click the **Create Profile** button. These profiles are kept within the **Stored Profiles** page linked from the left navigation bar.

— Once package profiles have been compared, Provisioning customers have the ability to synchronize the packages of the selected system with the package manifest of the compared profile. Note that this action may delete packages on the system not in the profile, as well as install packages from the profile. To install specific packages, select the checkboxes of packages from the profile. To remove specific packages already installed on the system itself, select the checkboxes of packages showing a difference of "This system only." To synchronize the system's packages with the compared profile entirely, select the master checkbox at the top of the column. Then click the **Sync Packages to** button. On the confirmation screen, review the changes, select a time frame for the action, and click the **Schedule Sync** button.

#### *6.4.2.6.4. System Details ⇒ Channels*

Manage the channels associated with the system.

##### *6.4.2.6.4.1. System Details ⇒ Channels ⇒ Software*

Software channels provide a well-defined method to determine which packages should be available to a system for installation or upgrade, based upon its operating systems, packages and, functionality. Click a channel name to view its **Channel Details** page. To modify the child channels associated with this system, use the checkboxes next to the channels and click the **Change Subscriptions** button. You will receive a success message or be notified of any errors. To change the system's base channel, select the new one from the pulldown menu and click the **Modify Base Channel** button. Refer to Section 6.6.1 *Software Channels* for more information.

##### *6.4.2.6.4.2. System Details ⇒ Channels ⇒ Configuration —*

Assists in managing the configuration of the system. This section is available to normal users with access to systems that have configuration management enabled. Like software channels, configuration channels store files to be installed on systems. While software updates are provided by RHN, configuration files are managed solely by you. Also unlike software packages, various versions of configuration files may prove useful to a system at any given time. Remember, only the latest version can be deployed. If you want to distribute an older version through RHN, make it the latest version first.

To manage the configuration of a system, it must have the latest `rhncfg*` packages installed and the `configfiles/` directory and associated files created on it. Refer to Section 6.6.6.1 *Preparing Systems for Config Management* for instructions. Command line tools also exist for many of these functions. Refer to Appendix A *Command Line Config Management Tools* for instructions.

Here are the options available within the system's **Configuration** tab, each of which results in a separate subtab:

- **Managed Files** — List all configuration files currently associated with the system. The Overrides column identifies which config file from which channel will apply if the system is unsubscribed from the config channel that provides the file now. For instance, if a system has '/etc/foo' from channel 'bar' and '/etc/foo' from channel 'baz' is in the Overrides column, then unsubscribing from channel 'bar' will mean that the file from channel 'baz' will be applicable. Also, if nothing is in the 'Overrides' column for a given file path, then unsubscribing from the channel providing the file will mean that the file is no longer managed (though it will (*not* remove the file from the system).

- **Diff** — Validate the configuration files installed on the system by comparing them to versions stored in RHN's central configuration manager. Select the files to be diffed and click **Analyze Differences**.
- **Config Channels** — Set the subscription and rank of configuration channels that may be associated with the system, lowest first. Enter numbers in the **Rank** fields to establish the order in which channels are used. Channels with no numeric value are not associated with the system. This system's local configuration channel will always override all other channels for this system and therefore cannot have its rank adjusted from 1. All other channels are created in the **Manage Config Channels** interface within the **Channels** category. Refer to Section 6.6.6 *Manage Config Channels* — for instructions. When satisfied, click **Update**.
- **Local Overrides** — View and manage the default configuration files for the system. If no files exist, you may use the **add files**, **upload files**, and **add directories** links within the page description to associate files with this system. These tabs correspond to those within the **Configuration Channel Details** page, affecting your entire organization and available only to Configuration Administrators.

  Refer to Section 6.6.6.5 *Configuration Channel Details* — for instructions.

  If a file exists, click its name to go to the **Configuration File Details** page. Refer to Section 6.6.6.6 *Configuration File Details* — for instructions. To replicate the file within a config channel, select its checkbox, click the **Copy to Config Channel** button, and select the destination channel. To remove a file, select it and click **Delete Selected Files**.
- **Sandbox** — Manipulate configuration files without deploying them. This sandbox provides you with an area to experiment with files without affecting systems. To add files, click the **import new files** link, select an option for their addition from the dropdown menu, and click **Go**. Ensure you have the latest `rhncfg*` packages. The rest of the functions work like those on the **Local Overrides** subtab.

#### *6.4.2.6.5. System Details ⇒ Groups —*

Lists the system's associated groups and enables you to change these associations.

#### *6.4.2.6.5.1. System Details ⇒ Groups ⇒ List/Remove —*

Lists groups to which the system belongs and enables you to cancel those associations. Only System Group Administrators and Organization Administrators can remove the system from groups. Non-admins just see a 'Review this system's group membership' page. To remove the system from groups, select the groups' checkboxes and click the **Leave Selected Groups** button. Click on a group's name to go to its **System Group Details** page. Refer to Section 6.4.3.3 *System Group Details* — for more information.

#### *6.4.2.6.5.2. System Details ⇒ Groups ⇒ Join —*

Lists groups that the system may be subscribed to. Only System Group Administrators and Organization Administrators can add the system to groups. Non-admins just see a 'Review this system's group membership' page. To add the system to groups, select the groups' checkboxes and click the **Join Selected Groups** button.

#### 6.4.2.6.6. System Details ⇒ Snapshots —

Provides snapshots enabling rollback of the system's package profile, configuration files, and RHN settings. These snapshots are captured whenever an action takes place on the system.

##### 6.4.2.6.6.1. System Details ⇒ Snapshots ⇒ Snapshots —

The default display of the **Snapshots** tab lists the reason, dates, and times for snapshots taken, as well as any tags associated with the snapshots. To revert to a previous configuration, click the Reason of the snapshot taken at the desired date and time and review the potential changes on the provided subtabs, starting with **Rollback**.

You may add a tag to an existing snapshot on the **System Details** ⇒ **Snapshots** ⇒ **Snapshots** ⇒ **Snapshot Tags** subtab by clicking the **create new snapshot tag** link, providing a descriptive term, and clicking **Tag This Snapshot** button. Refer to Section 6.4.2.6.6.2 *System Details* ⇒ *Snapshots* ⇒ *Snapshot Tags* — for more information. When satisfied with the reversion, return to the **Rollback** subtab and click the **Rollback to Snapshot** button. To see the list again, click **Return to snapshot list**.

##### 6.4.2.6.6.2. System Details ⇒ Snapshots ⇒ Snapshot Tags —

Provides a means to add meaningful descriptions to your most recent system snapshot. This can be used to indicate milestones, such as a known working configuration or a successful upgrade. To tag the most recent snapshot, click **create new system tag**, enter a descriptive term in the **Tag name** field, and click the **Tag Current Snapshot** button. Refer to Section 6.4.2.6.6.1 *System Details* ⇒ *Snapshots* ⇒ *Snapshots* — to tag older snapshots. You may then revert using this tag directly by clicking its name in the Snapshot Tags list. To delete tags, select their checkboxes, click **Remove Tags**, and confirm the action.

#### 6.4.2.6.7. System Details ⇒ Kickstart —

Enables the re-installation of the system based upon selectable parameters, including specific Red Hat distribution. These kickstarts are based upon profiles developed within the **Kickstart** interface. Refer to Section 6.4.10 *Kickstart* — for details.

##### 6.4.2.6.7.1. System Details ⇒ Kickstart ⇒ Schedule —

The default display of the **Kickstart** tab, this subtab allows the kickstarting of the selected system. To schedule a kickstart, select a distribution, identify the type (IP address or manual selection of kickstart profile), and click **Continue**. Note that IP address kickstarts require ranges to be defined in kickstart profiles.

On the next page, finish choosing from the options available. Using the existing RHN profile will rely upon the system-specific activation key created within the **Reactivation** tab to reregister the system. *Do not regenerate, delete, or use this key while a profile-based kickstart is in progress.* Selecting the **Deploy Configuration** checkbox will re-install configuration files from any config channels associated with the system. When finished, click the **Schedule Kickstart** button.

**Caution**

It is imperative the kickstart profile selected match the installation files supplied. For instance, it is possible a given IP address could be associated with a Red Hat Enterprise Linux 2.1 kickstart profile,

but you insert an IP address kickstart CD-ROM built for Red Hat Enterprise Linux 3. This would result in errors and cause the kickstart to fail.

#### *6.4.2.6.7.2. System Details ⇒ Kickstart ⇒ Session Status* —

If you've scheduled a kickstart, this subtab shows where the system's kickstart stands. Details include the kickstart profile used, its state, and pending and latest actions. Kickstarts that do not complete within approximately two hours will be marked as failed here. Click the profile name to access the **Kickstart Details** page. Click the **view** link to see the actual kickstart configuration file generated by RHN. To force this page to reload at a set interval, select one from the pulldown menu and click the **Change Reload Time** button.

#### *6.4.2.6.7.3. System Details ⇒ Kickstart ⇒ Session History* —

Displays particular points in a kickstart session's progress. Like **Session Status**, this subtab appears only if you've scheduled a kickstart. It lists individual actions, such as package installs, as they occur. Click the name of an action to see information about it, including summary, details, and time. Failed kickstarts are shown here, as well. To force this page to reload at a set interval, select one from the pulldown menu and click the **Change Reload Time** button.

### *6.4.2.6.8. System Details ⇒ Events*

Displays past, current, and scheduled actions on the system. You may cancel pending events here. The following sections describe the **Events** subtabs and the features they offer.

#### *6.4.2.6.8.1. System Details ⇒ Events ⇒ History*

The default display of the **Events** tab lists the type and status of events that have failed, occurred or are occurring. To view details of an event, click its summary in the **System History** list. To again view the table, click **Return to history list** at the bottom of the page.

#### *6.4.2.6.8.2. System Details ⇒ Events ⇒ Pending*

Lists events that are scheduled but have not begun. A prerequisite action is required to complete successfully before a given action will be attempted. If an action has a prerequisite, there will not be a checkbox available to cancel that specific action. Instead, there will be a checkbox next to the prerequisite action; Cancelling the prerequisite action will cause the action in question to fail.

Actions can be chained in this manner so that action 'a' requires action 'b' which requires action 'c'. Action 'c' will be the first one attempted, and will be the one with the checkbox next to it until it is completed successfully - if any action in the chain fails, the remaining actions also fail. To unschedule a pending event, select the event and click the **Cancel Events** button at the bottom of the page. The following icons indicate the type of events listed here:

- — Package Event
- — Errata Event
- — Preferences Event

- — System Event

#### *6.4.2.6.9. System Details ⇒ Probes —*

Displays all of the probes monitoring the system. You must be logged into an RHN Satellite Server with Monitoring enabled to see this tab. The **State** column shows icons representing the status of each probe. Refer to Section 6.9 *Monitoring —* for descriptions of these states. The **Status String** column displays the last message received from the probe. Clicking the probe description takes you to its **Current State** page.

To add a probe to the system, click the **create new probe** link at the top-right corner of the page and complete the fields on the following page. Refer to Section 7.3.1 *Creating Notification Methods* for detailed instructions.

Once the probe has been added, you must reconfigure your Monitoring infrastructure to recognize it. Refer to Section 6.9.3 *Scout Config Push —* for details. After the probe has run, its results become available on the **Current State** page. Refer to Section 6.9.1.7 *Current State —* for details.

### 6.4.3. System Groups —

The **System Groups** page allows all RHN Management and Provisioning users to view the **System Groups** list. Only System Group Administrators and Organization Administrators may perform the following additional tasks:

1. Create system groups. (Refer to Section 6.4.3.1 *Creating Groups*.)
2. Add systems to system groups. (Refer to Section 6.4.3.2 *Adding and Removing Systems in Groups*.)
3. Remove systems from system groups. (Refer to Section 6.4.2.6 *System Details*.)
4. Assign system group permissions to users. (Refer to Section 6.8 *Users —* .)

As shown in Figure 6-4, the **System Groups** list displays all of your system groups.

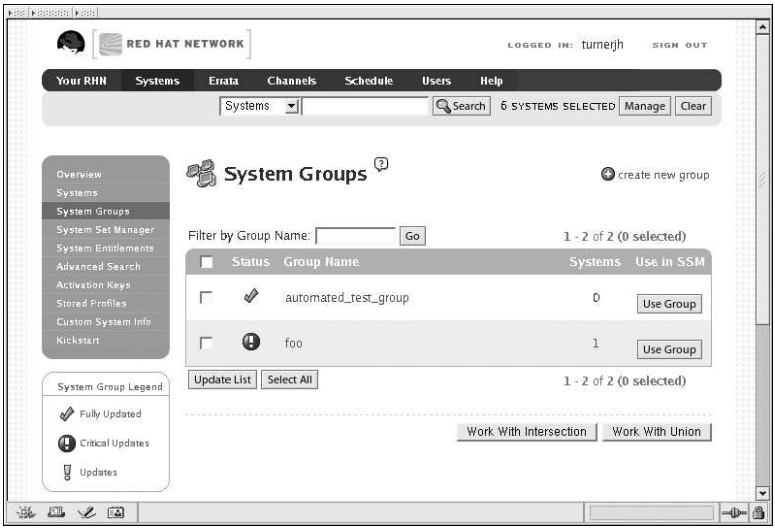


**Figure 6-4. System Group List**

The **System Groups** list contains several columns for each group:

- **Select** — These checkboxes enable you to add systems in groups to the **System Set Manager**. To select groups, mark the appropriate checkboxes and click the **Update** button below the column. All systems in the selected groups are added to the **System Set Manager**. You can then use the **System Set Manager** to perform actions on them simultaneously. To add only the systems in all selected groups, select them and click the **Work with Intersection** button. To add all systems in all selected groups, select them and click the **Work with Union** button. Each system will show up once, regardless of the number of groups to which it belongs. Refer to Section 6.4.4 *System Set Manager* — for details.
- **Status** — Shows which type of Errata Alerts are applicable to the group or confirms that it is up-to-date. Clicking on a group's status icon takes you to the **Errata** tab of its **System Group Details** page. Refer to Section 6.4.3.3 *System Group Details* — for more information.

  The status icons call for differing degrees of attention:

  - — All systems within group are up-to-date
  - — Critical Errata available, update *strongly* recommended
  - — Updates available and recommended

- **Group Name** — The name of the group as configured during its creation. The name should be explicit enough to easily differentiate between it and other groups. Clicking on the name of a group takes you to **Details** tab of its **System Group Details** page. Refer to Section 6.4.3.3 *System Group Details* — for more information.

- **Systems** — Total number of systems contained by the group. Clicking on the number takes you to the **Systems** tab of the **System Group Details** page for the group. Refer to Section 6.4.3.3 *System Group Details* — for more information.
- **Use in SSM** — Clicking the **Use Group** button in this column loads the group from that row and launches the **System Set Manager** immediately. Refer to Section 6.4.4 *System Set Manager* — for more information.

#### 6.4.3.1. Creating Groups

To add a new system group, click the **create new group** button at the top-right corner of the page. Type a name and description and click the **Create Group** button. Make sure you use a name that clearly sets this group apart from others. The new group will appear in the **System Groups** list.

#### 6.4.3.2. Adding and Removing Systems in Groups

Systems can be added and removed from system groups in two places: the **Target Systems** tab of the **System Group Details** page and the **Groups** tab of the **System Details** page. The process is similar in both instances. Select the systems to be added or removed and click the **Add Systems** or **Remove Systems** button.

#### 6.4.3.3. System Group Details —

At the top of each **System Group Details** page are two links: **work with group** and **delete group**. Clicking **delete group** does just that and should be used with caution. Clicking **Work with Group** functions similarly to the **Use Group** button from the **System Groups** list in that it loads the group's systems and launches the **System Set Manager** immediately. Refer to Section 6.4.4 *System Set Manager* — for more information.

The **System Group Details** page is broken down into tabs:

##### *6.4.3.3.1. System Group Details ⇒ Details* —

Basic information about the system group: the group name and group description. To change this information, click **Edit Group Properties**, make your changes in the appropriate fields, and click the **Modify Details** button.

##### *6.4.3.3.2. System Group Details ⇒ Systems* —

List of systems that are members of the system group. Clicking links within the table takes you to corresponding tabs within the **System Details** page for the associated system. To remove systems from the group, select the appropriate checkboxes and click the **Remove from group** button on the bottom of the page. Clicking it does not delete systems from RHN entirely. This is done through the **System Set Manager** or **System Details** pages. Refer to Section 6.4.4 *System Set Manager* — or Section 6.4.2.6 *System Details*, respectively.

##### *6.4.3.3.3. System Group Details ⇒ Target Systems* —

**Target Systems** — List of all systems in your organization. This tab enables you to add systems to the specified system group. Merely select the systems using the checkboxes to the left and click the **Add Systems** button on the bottom right-hand corner of the page.

#### *6.4.3.3.4. System Group Details ⇒ Errata —*

List of relevant Errata for systems in the system group. Clicking the Advisory takes you to the **Details** tab of the **Errata Details** page. (Refer to Section 6.5.2.2 *Errata Details* for more information.) Clicking the Affected Systems number lists all of the systems addressed by the Errata. To apply the Errata Updates in this list, select the systems and click the **Apply Errata** button.

#### *6.4.3.3.5. System Group Details ⇒ Admins —*

List of all organization users that potentially have permission to manage the system group. Organization Administrators are clearly identified. System Group Administrators are marked with an asterisk (*). To change the system group's users, select and unselect the appropriate checkboxes and click the **Update** button.

### 6.4.4. System Set Manager —

The **System Set Manager** allows you to perform many actions possible individually through the **System Details** page on multiple systems at once, including:

- Apply Errata updates
- Upgrade packages to the most recent versions available
- Add/remove systems to/from system groups
- Subscribe/unsubscribe systems to/from channels
- Update system profiles
- Modify system preferences such as scheduled download and installation of packages
- Kickstart several Provisioning-entitled systems at once
- Set the subscription and rank of configuration channels for Provisioning-entitled systems
- Tag the most recent snapshots of your selected Provisioning-entitled systems
- Revert Provisioning-entitled systems to previous snapshots
- Run remote commands on Provisioning-entitled systems

Before performing actions on multiple systems, you must select the systems you wish to modify. Note that Update-level systems cannot be selected. Pages including **Systems** list and **System Search** have a column of checkboxes under the **Select** heading. Mark the checkboxes beside the systems you want to select, and click the **Update List** button below the column to add them to the **System Set Manager**.

You can access the **System Set Manager** page in three ways: 1)The **System Set Manager** button in the left navigation bar. 2)The **Use Group** button in the **System Groups** list (or **Work with Group** on the **System Group Details** page to work). 3)The **Manage** button just below the top navigation bar. The **System Set Manager** page is broken down into tabs:

#### 6.4.4.1. System Set Manager ⇒ Overview —

Description of the various options available to you in the remaining tabs.

#### 6.4.4.2. System Set Manager ⇒ Systems —

List of systems now selected. To remove systems from this set, select them and click the **Remove** button.

#### 6.4.4.3. System Set Manager ⇒ Errata —

List of Errata Updates applicable to the current system set. Click the number in the Systems column to see to which systems in the System Set Manager the given Errata applies to. To apply updates, select the Errata and click the **Apply Errata** button.

#### 6.4.4.4. System Set Manager ⇒ Packages —

Options to modify packages on the system within the following subtabs (Click the number in the Systems column to see to which systems in the System Set Manager the given package applies to.):

— When selecting packages to install, upgrade, or remove, Provisioning customers have the option of running a remote command automatically before or after the package installation. Refer to Section 6.4.2.6.1.7 *System Details ⇒ Details ⇒ Remote Command* — for more information.

##### *6.4.4.4.1. System Set Manager ⇒ Packages ⇒ Install* —

A list of channels from which you may retrieve packages. The list of channels is the list of all the channels that systems in the set are subscribed to; a package will be installed on a system only if the system is subscribed to the channel from which the package comes. Click on the channel name and select the packages from the list. Then click the **Install Packages** button.

##### *6.4.4.4.2. System Set Manager ⇒ Packages ⇒ Upgrade* —

A list of all the packages installed on the selected systems that might be upgraded. Systems must be subscribed to a channel providing the package for the system to be able to upgrade the package. If multiple versions of a package appear, note that only the latest version available to each system will be upgraded on that system. Select the packages to be upgraded, then click the **Upgrade Packages** button.

##### *6.4.4.4.3. System Set Manager ⇒ Packages ⇒ Remove* —

A list of all the packages installed on the selected systems that might be removed. Multiple versions will appear if systems in the System Set Manager have more than one version installed. Select the packages to be deleted, then click the **Remove Packages** button.

#### 6.4.4.5. System Set Manager ⇒ Groups —

Tools to create groups and manage group membership. These functions are limited to Organization Administrators and System Group Administrators. To add a new group, click **create new group** on the top-right corner. In the resulting page, type its name and description in the identified fields and click the **Create Group** button. To add or remove the selected systems in any of the system groups, toggle the appropriate radio buttons and click the **Alter Membership** button.

#### 6.4.4.6. System Set Manager ⇒ Channels —

Options to manage channel associations through the following subtabs:

##### *6.4.4.6.1. System Set Manager ⇒ Channels ⇒ Channel Subscriptions —*

To subscribe or unsubscribe the selected systems in any of the channels, toggle the appropriate radio buttons and click the **Alter Subscriptions** button. Keep in mind, subscribing to channels uses up channel entitlements, and if not enough channel entitlements are available, not all systems will get an entitlement. Similarly, systems will be subscribed to a child channel only if they are subscribed to the base channel that is the parent of the child channel in question.

##### *6.4.4.6.2. System Set Manager ⇒ Channels ⇒ Config Channels —*

Like the options within the **System Details** ⇒ **Channels** ⇒ **Configuration** tab, the subtabs here can be used to subscribe the selected systems to configuration channels and deploy and compare the configuration files on the systems. The channels are created in the **Manage Config Channels** interface within the **Channels** category. Refer to Section 6.6.6 *Manage Config Channels* — for channel creation instructions.

To manage the configuration of a system, it must have the latest `rhncfg*` packages installed and the `configfiles/` directory and associated files created on it. Refer to Section 6.6.6.1 *Preparing Systems for Config Management* for instructions. Command line tools also exist for many of these functions. Refer to Appendix A *Command Line Config Management Tools* for instructions.

##### *6.4.4.6.2.1. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Subscriptions —*

On this subtab, available only to Configuration Administrators and Organization Administrators, enter numbers in the Rank column to establish the order in which channels are used, lowest first. Channels not assigned a numeric value will not be associated with the systems. Your local configuration channel will always override all other channels. Once you've established the rank of the config channels, you must decide how they should be applied to the selected systems.

The three buttons below the channels reflect your options. Clicking **Add with Highest Rank** places all the ranked channels before any channels already subscribed to by the systems. Clicking **Add with Lowest Rank** places the ranked channels after channels subscribed to by the systems. Clicking **Replace Existing Config Channels** removes any existing association and starts cleanly with the ranked channels, leaving every system with the same config channels in the same order.

In the first two cases, if any of the newly ranked config channels is already in a system's existing config channel list, the duplicate channel is removed and re-added according to the new rank, effectively reordering the system's existing channels. When such conflicts exist, you're presented with a confirmation page to ensure the intended action is correct. When the change has taken place, a message appears at the top of the page indicating the update was successful.

##### *6.4.4.6.2.2. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Deploy —*

Use this subtab to distribute configuration files from your central repository on RHN to the selected systems at once. The table lists the configuration files associated with any of the selected systems. Clicking its system count displays the systems already subscribed to the file.

To subscribe the selected systems to the available configuration files, select the checkbox for each desired file. When done, click **Deploy Configuration** and schedule the action. Note that the files deployed are of the latest version at the time of scheduling and do not account for versions that may appear before the action takes place.

#### *6.4.4.6.2.3. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Diff —*

Use this subtab to validate configuration files on the selected systems against copies in your central repository on RHN. The table lists the configuration files associated with any of the selected systems. Clicking its system count displays the systems already subscribed to the file.

To compare the configuration files deployed on the systems with those in RHN, select the checkbox for each file to be validated. Then click **Analyze Differences** and schedule the action. Note that the files compared are of the latest version at the time of scheduling and do not account for versions that may appear before the action takes place. Then find the results within the main **Schedule** category or within the **System Details** ⇒ **Events** tab.

#### *6.4.4.6.3. System Set Manager ⇒ Channels ⇒ Base Channel Alteration —*

Channel Administrators may use this subtab to change the base channels the selected systems are subscribed to. The default Red Hat base channel selection in the pulldown menu will subscribe the system to whichever Red Hat-provided base channel representing the operating system installed on the system. Systems will be unsubscribed from all channels and subscribed to the new base channels. For this reason, this should be done with caution. Select the new base channel from the pulldown menus and click the **Change Base Channels** button.

### 6.4.4.7. System Set Manager ⇒ Provisioning — 

**Provisioning** — Options for provisioning systems through the following subtabs:

#### *6.4.4.7.1. System Set Manager ⇒ Provisioning ⇒ Kickstart —*

Use this subtab to re-install the selected Provisioning-entitled systems. To schedule a kickstart, select a distribution, identify the type (IP address or manual), and click **Continue**. Then finish choosing from the options available on the subsequent screen and click the **Schedule Kickstart** button.

#### *6.4.4.7.2. System Set Manager ⇒ Provisioning ⇒ Tag Systems —*

Use this subtab to to add meaningful descriptions to the most recent snapshots of your selected systems. To tag the most recent system snapshots, enter a descriptive term in the **Tag name** field, and click the **Tag Current Snapshots** button.

#### *6.4.4.7.3. System Set Manager ⇒ Provisioning ⇒ Rollback —*

Use this subtab to rollback selected Provisioning-entitled systems to previous snapshots marked with a tag. Click the name of the tag, verify the systems to be reverted, and click the **Rollback Systems** button.

#### *6.4.4.7.4. System Set Manager ⇒ Provisioning ⇒ Remote Command —*

Use this subtab to issue remote commands on selected Provisioning-entitled systems. You must have created a `run` file on the client systems for this function to be allowed. Refer to the description of the **Configuration** subtab of the **Channels** tab for instructions. You may then identify a specific user,

group, and timeout period, as well as the script itself on this page. Select a date and time to begin attempting the command, and click **Schedule Remote Command**.

#### 6.4.4.8. System Set Manager ⇒ Misc —

**Misc** — Tools to update System Profiles and preferences for the system set. Here are the tools broken down by section:

##### *6.4.4.8.1. System Set Manager ⇒ Misc ⇒ System Profile Updates* —

Clicking **Update Hardware Profile**, then the **Confirm Refresh** button schedules a hardware profile update. Clicking **Update Package Profile**, then the **Confirm Refresh** button schedules a package profile update.

##### *6.4.4.8.2. System Set Manager ⇒ Misc ⇒ Custom System Information* —

Clicking **Set a custom value** then the name of a key allows you to provide values for all selected systems. Enter the information and click the **Set Values** button. Clicking **Remove a custom value** then the name of a key allows you to remove values for all selected systems. Click the **Remove Values** button to finalize the deletion.

##### *6.4.4.8.3. System Set Manager ⇒ Misc ⇒ Reboot Systems* —

Selecting the appropriate systems and then clicking the **Reboot Systems** link sets those systems for reboot. To immediately cancel this action, click the **list of systems** link that appears within the confirmation message at the top of the page, select the systems, and click **Unschedule Action**.

##### *6.4.4.8.4. System Set Manager ⇒ Misc ⇒ Lock Systems* —

Selecting the appropriate systems and then clicking the **Lock Systems** link prevents the scheduling of any action through RHN that would affect the systems. This can be reversed by clicking the **Unlock Systems** link.

##### *6.4.4.8.5. System Set Manager ⇒ Misc ⇒ Delete Systems* —

Clicking **Delete System Profiles**, then the **Confirm Deletions** button removes the selected profiles permanently.

##### *6.4.4.8.6. System Set Manager ⇒ Misc ⇒ Upgrade System Entitlements* —

Clicking **Upgrade to * Entitlement** upgrades the entitlement for as many selected systems as possible. Keep in mind, entitlements cannot be downgraded.

#### *6.4.4.8.7. System Set Manager ⇒ Misc ⇒ System Preferences —*

Toggling the **Yes** and **No** radio buttons and then clicking the **Change Preferences** button alters your notification preferences for the selected systems. All of these preferences may also be applied to systems individually through the **Properties** subtab of the **System Details** page. Refer to Section 6.4.2.6.1.2 *System Details ⇒ Details ⇒ Properties* for instructions.

- **Receive Notifications of Updates/Errata** — This setting keeps you abreast of all advisories pertaining to your systems. Anytime an update is produced and released for a system under your supervision, a notification is sent via email.
- **Include system in Daily Summary** — This setting includes the selected systems in a daily summary of system events. (By default, all Management and Provisioning systems are included in the summary.) These are actions affecting packages, such as scheduled Errata Updates, and system reboots or failures to check in. In addition to including the systems here, you must choose to receive email notifications in the **Your Preferences** page of the **Your RHN** category. Refer to Section 6.3.2 *Your Preferences* for instructions. Note that RHN will send these summaries only to verified email addresses.
- **Automatic application of relevant Errata** — This setting allows you have all Errata Updates automatically applied to systems. This means packages associated with Errata will be updated without any user intervention. Customers should note that Red Hat does not recommend the use of the auto-update feature for production systems because conflicts between packages and environments can cause system failures.

### 6.4.5. System Entitlements

To use all of the features of RHN, your systems must be *entitled* — subscribed to an RHN service level. Use the **System Entitlements** page to configure which systems are entitled to which service offerings. There are three primary types of entitlements:

- **Update** — should be used to manage a single Red Hat Enterprise Linux system. It includes Errata Alerts, Scheduled Errata Updates, Package Installation, and the **Red Hat Update Agent**.
- **Management** — should be used to manage multiple systems with multiple system administrators. In addition to the features of the Update offering, it includes system group management, user management, and the **System Set Manager** interface to quickly perform actions on multiple systems.
- **Provisioning** — offers the highest level of functionality. It should be used to provision multiple systems that will need to be re-installed and reconfigured regularly. The Provisioning offering provides tools for kickstarting machines, managing their configuration files, conducting snapshot rollbacks, and inputting searchable custom system information, as well as all of the functionality included in the Management service level.

The **System Entitlements** page allows you to view and promote the entitlements for your registered systems. Only increases in entitlement levels are allowed. Systems cannot be re-entitled to a lower entitlement level. For instance, a system entitled to the Update service level can be promoted to the Management level, but this action cannot be reversed.

To change an individual entitlement, select the entitlement from the system's pulldown menu and click the **Update Entitlements** button on the bottom right-hand corner of the page. Click the name of a system to see details about it. If no drop-down menu exists for your Update-level system, you may need to purchase a Management entitlement. Do this through the **Buy Now** link at the left of the page.

**Warning**

Changing a system's entitlement is an irreversible action. You may be unable to change the entitlement levels of some systems. For more information, refer to the RHN entitlement policy linked from the **System Entitlements** page.

In addition, you may entitle all newly registered systems to the Management service level at once by clicking the **Auto-Entitle Newest Servers Now** link at the bottom of the page. To use this link, which appears only when new, unentitled systems exist, first make sure you have enough Management entitlements available. If you need to purchase additional entitlements, click the **Buy more system entitlements now** link at the top of the page. After auto-entitling, a message appears at the top of the **System Entitlements** page indicating the number of systems successfully entitled to the Management service level.

When an entitlement expires, the last system entitled to the same service level (such as Management) will be unentitled. For instance, if you have 10 Red Hat Enterprise Linux AS systems entitled to Management and either one of the RHN entitlements or one of the operating system subscriptions expire, the last system subscribed or entitled will have their subscription or entitlement removed.

## 6.4.6. Advanced Search —

The **System Search** page allows you to search through your systems according to specific criteria. These criteria include custom system information, system details, hardware, devices, interface, networking, packages, and location. The activity selections (Days Since Last Checkin, for instance) can be especially useful in finding and removing outdated System Profiles. Type the keyword, select the criterion to search by, use the radio buttons to identify whether you wish to query all systems or only those loaded in the **System Set Manager**, and click the **Search** button. Yo may also select the **Invert Result** checkbox to list those systems that do *not* match the criteria selected.

The results appear at the bottom of the page. For details about using the resulting system list, refer to Section 6.4.2 *Systems*.

## 6.4.7. Activation Keys —

RHN Management and Provisioning customers with the Activation Key Administrator role (including Organization Administrators) can generate activation keys through the RHN website. These keys can then be used to register a Red Hat Enterprise Linux system, entitle the system to an RHN service level and subscribe the system to specific channels and system groups through the command line utility `rhnreg_ks`. Refer to Section 2.5 *Registering with Activation Keys* for instructions on use.

**Note**

System-specific activation keys created through the **Reactivation** subtab of the **System Details** page do not show up in this list because they are not reusable across systems.

### 6.4.7.1. Managing Activation Keys

To generate an activation key:

1. Select **Systems => Activation Keys** from the top and left navigation bars.

2. Click the **create new key** link at the top-left corner.

**Warning**

In addition to the fields listed below, RHN Satellite Server customers may also populate the **Key** field itself. This user-defined string of characters can then be supplied with `rhnreg_ks` to register client systems with the Satellite. *Do not insert commas in the key.* All other characters are accepted. Commas are problematic since they are the separator used when including two or more activation keys at once. Refer to Section 6.4.7.2 *Using Multiple Activation Keys at Once* — for details.

3. Provide the following information:

- **Description** — User-defined description to identify the generated activation key.
- **Usage Limit** — The number of times the key can be used to register a system before the activation key is disabled. Leave blank for unlimited use.
- **Base Channel** — The primary channel for the key. Selecting nothing will enable you to select from all child channels, although systems can be subscribed to only those that are applicable.
- **Entitlement** — The service level for the key, either Management or Provisioning. All systems will be subscribed at this level with the key.
- **Universal default** — Whether or not this key should be considered the primary activation key for your organization.

Click **Create Key**.

After creating the unique key, it appears in the list of activation keys along with the number of times it has been used. Note that only Activation Key Administrators can see this list. At this point, you may associate child channels and groups with the key so systems registered with it will automatically be subscribed to them.

To change information about a key, such as the channels or groups, click its description in the key list, make your modifications in the appropriate tab, and click the **Update Key** button. To disassociate channels and groups from a key, deselect them in their respective menus by [Ctrl]-clicking their highlighted names. To remove a key entirely, click the **delete key** link in the top-right corner of the edit page.

If you do not want a key to be used to activate a system, you can disable it by unselecting the corresponding checkbox under the **Enabled** column in the key list. The key can be re-enabled by selecting the checkbox. After making these changes, click the **Update Keys** button on the bottom right-hand corner of the page.

### 6.4.7.2. Using Multiple Activation Keys at Once —

Provisioning customers should note that multiple activation keys can be included at the command line or in a single kickstart profile. This allows you to aggregate the aspects of various keys without having to recreate a new key specific to the desired systems, simplifying the registration and kickstart processes while slowing the growth of your key list.

Without this stacking ability, your organization would need at least six activation keys to manage four server groups and subscribe a server to any two groups. Factor in two versions of the operating system, such as Red Hat Enterprise Linux 2.1 and 3, and you need twice the number of activation keys. A larger organization would need keys in the dozens.

Before specifiying more than one activation key, you must understand how their values are combined and resolved. These entities are straight unions: server groups, software packages, software child channels, and config channels. A combination of these will be used. If there is a conflict between the remaining properties, they will be resolved in the following manner:

- base software channels — registration fails
- entitlements — registration fails
- enable config flag — configuration management is set

Also remember, using a system-specific re-activation key along with a normal activation key will fail.

You're now ready to use multiple activation keys at once. This is done with comma separation at the command line with `rhnreg_ks` or in a kickstart profile within the **Post** tab of the **Kickstart Details** page. Refer to Section 2.5 *Registering with Activation Keys* and Section 6.4.10.3 *Creating Kickstarts*, relatively, for instructions.

### 6.4.8. Stored Profiles —

RHN Provisioning customers can create package profiles through the **Profiles** subtab of the **Packages** tab within the **System Details** page. Those profiles end up here, on the **Stored Profiles** page, where they may be edited and even deleted.

To edit a profile, click its name in the list, alter its name and description, and click the **Update Profile**. To view software associated with the profile, click the **Packages** subtab. To remove the profile entirely, click **delete stored profile** at the upper-right corner of the page.

### 6.4.9. Custom System Info —

RHN Provisioning customers may include completely customizable information about systems. Unlike notes, the information here is more formal and can be used in searches. For instance, you may decide to identify an asset tag for each system. To do this, you must create an **`asset`** key within the **Custom System Info** page.

Click **create new key** at the upper-right corner of the page. Enter a descriptive label and description, such as **`Asset`** and **`Precise location of each system`**, and click the **Create Key**. The key will then show up in the custom info keys list.

Once the key exists, you may assign a value to it through the **Custom Info** tab of the **System Details** page. Refer to Section 6.4.2.6.1.5 *System Details* ⇒ *Details* ⇒ *Custom Info* — for instructions.

### 6.4.10. Kickstart —

To satisfy the provisioning needs of customers, RHN provides this interface for developing kickstart profiles that can be used to install Red Hat Enterprise Linux on either new or already-registered systems. This enables systems to be installed to particular specifications automatically.

**Important**

If your systems are connected to the central RHN Servers, you will need an external installation tree for each distribution to be kickstarted. This tree can be hosted anywhere that is accessible by the target system via HTTP. If the systems are connected through an RHN Proxy Server, then you may place the installation tree in `/var/www/html/pub/` on the Proxy. RHN Satellite Servers already have a tree for each Red Hat distribution and therefore do not require separate trees. Even if the system connects through an RHN Proxy Server to get to the Satellite, these trees will be available for kickstart. Refer to Section 6.4.10.9 *Kickstart* ⇒ *Distributions* — for instructions on setting up installation trees.

#### 6.4.10.1. Kickstart Prerequisites

Although Red Hat Network has taken great pains to ease the provisioning of systems, some preparation is still required for your infrastructure to handle kickstarts. For instance, before creating kickstart profiles, you may consider:

- A DHCP server is not required for kickstarting, but it can make things easier. If you are using static IP addresses, you should select static IP while developing your kickstart profile.
- An FTP server can be used in place of hosting the kickstart distribution trees via HTTP.
- If conducting a bare metal kickstart, you should 1)Configure DHCP to assign required networking parameters and the bootloader program location. 2)Specify within the bootloader configuration file the kernel to be used and appropriate kernel options.

For a decription of the innerworkings of the kickstart process, refer to Section 6.4.10.2 *Kickstart Explained*.

#### 6.4.10.2. Kickstart Explained

When a machine is to receive a network-based kickstart, the following events must occur in this order:

1. After being placed on the network and turned on, the machine's PXE logic broadcasts its MAC address and a request to be discovered.
2. If a static IP address is not being used, the DHCP server recognizes the discovery request and extends an offer of network information needed for the new machine to boot. This includes an IP address, the default gateway to be used, the netmask of the network, the IP address of the TFTP or HTTP server holding the bootloader program, and the full path and filename of that program (relative to the server's root).
3. The machine applies the networking information and initiates a session with the server to request the bootloader program.
4. The bootloader, once loaded, searches for its configuration file on the server from which it was itself loaded. This file dictates which kernel and kernel options, such as the initial RAM disk (initrd) image, should be executed on the booting machine. Assuming the bootloader program is SYSLINUX, this file will be located in the `pxelinux.cfg` directory on the server and named the hexadecimal equivalent of the new machine's IP address. For example, a bootloader configuration file for Red Hat Enterprise Linux AS 2.1 should contain:
```
port 0
prompt 0
timeout 1
default My_Label
label My_Label
       kernel vmlinuz
       append ks=http://myrhnsatellite/ initrd=initrd.img network apic
```
5. The machine accepts and uncompresses the init image and kernel, boots the kernel, and initiates a kickstart installation with the options supplied in the bootloader configuration file, including the server containing the kickstart configuration file.
6. This kickstart configuration file in turn directs the machine to the location of the installation files.
7. The new machine is built based upon the parameters established within the kickstart configuration file.

#### 6.4.10.3. Creating Kickstarts

To develop a new kickstart profile, and you are not using RHN Satellite Server, first create a distribution through the **Distributions** page. Refer to Section 6.4.10.9 *Kickstart ⇒ Distributions —* for instructions. Once that is done, return to the **Kickstart** page and click **create new kickstart** in the upper-right corner of the page. On the resulting page, enter a name and label for the profile, select whether it should immediately be considered active, and click the **Select Kickstart Options** button.

On the next page, identify the precise values to be included in the profile, including: bootloader type, time zone, kickstart network configuration, root password, and partition details. Please note that the kickstart network configuration value here is different from the network setting on the **Advanced Options** tab. Refer to the individual tab descriptions for details. Click the **Create Kickstart** button when done.

When finished with the initial profile, you're presented with the **Kickstart Details** page, which offers various options for enhancing the kickstart steps. Refer to Section 6.4.10.4 *Kickstart Details —* for descriptions of the page and its tabs. Take note that RHN supports including separate files within the Partition Details section of the kickstart profile. For instance, you may dynamically generate a partition file based on the machine type and number of disks at kickstart time. This file can be created via %pre script and placed on the system, such as `/tmp/part-include`. Then you can call for that file by including the following line within the Partition Details field of the **Kickstart Details ⇒ Options** tab:

```
%include /tmp/part-include
```

You may clone or delete the profile at any time using links at the upper-right corner of the **Kickstart Details** page. Once you've populated the tabs and fields within the **Kickstart Details** page, the kickstart profile should be completely configured and ready for use. Refer to the following pages for instructions on supplementing and aggregating kickstart profiles.

#### 6.4.10.4. Kickstart Details —

Use the following tabs to modify the kickstart profile.

##### *6.4.10.4.1. Kickstart Details ⇒ Details —*

The default display of the **Kickstart Details** page shows the kickstart profile name and label, as well as the associated distribution, URL to be used, whether it's the default profile for your organization, and any comments about the profile. The URL for a kickstart is used when creating a bootable CD-ROM image that will kickstart a system using this profile. Note that the URL does not begin with `https://` because the Red Hat Enterprise Linux installation program does not support Secure Sockets Layer (SSL). Click the **view kickstart** link to see the actual kickstart configuration file (converted to SSL) generated by RHN.

In addition, you may select lists of files here that will be preserved during the kickstart process. These files, typically configuration files and others that will remain relevant when the server is re-deployed, can be selected using the File Preservation Lists pulldown menu near the bottom of the page. Refer to Section 6.4.10.10 *Kickstart ⇒ File Preservation —* to find out how create these lists. To deselect a list, hold the [Ctrl] key and click the list name with the mouse. When done, click the **Update Kickstart** button.

#### *6.4.10.4.2. Kickstart Details ⇒ Options* —

Collects the precise values to be applied against the kickstart process, including bootloader type, time zone, root password, and partition details. Keep in mind, the kickstart network configuration value here is used by the bootloader to determine the network configuration for the kickstart process, unlike the network setting on the **Advanced Options** tab, which is used to generate the kickstart configuration file. The options passed to the bootloader are different from those needed by the Red Hat installation program to configure the system. Remember you may **`%include`** separate files in the Partition Details section of the profile if needed. When done, click the **Update Kickstart** button.

#### *6.4.10.4.3. Kickstart Details ⇒ Advanced Options* —

Accessible through a link at the top of the **Options** tab, this page establishes the arguments to be included in the kickstart configuration file. These differ from the settings included on the **Options** tab. For instance, the network setting here defines the parameters of the Red Hat installation program (Anaconda), while the kickstart network configuration value there affects the bootloader. (Note that these options are passed to Anaconda with little or no verification for correctness. As an example, you might need to kickstart a system using eth1 (kickstart network configuration), but eth0 is the primary network interface for the box (as identified in the network field on this page). When done, click the **Update Kickstart** button.

#### *6.4.10.4.4. Kickstart Details ⇒ Packages* —

Allows the addition or removal of specific software packages from the kickstart profile. To include packages, enter them in the text field. These are passed directly to Anaconda. To remove packages, precede them with with a dash (-). You may also enter entire components and exclude specific packages, such as **`@ X Window System`** and **`-filename.rpm`**.

Note that packages to be excluded may still be installed to resolve dependencies and ensure the system works properly. When finished, click **Add Packages**. To delete packages from the list you've created, enter them below and click **Remove Packages**.

#### *6.4.10.4.5. Kickstart Details ⇒ Pre* —

Enables you to edit the %pre script for the kickstart profile. Make your changes and click the **Update Pre** button.

#### *6.4.10.4.5.1. Kickstart Details ⇒ Pre ⇒ --interpreter* —

Enables you to specify an interpreter and specific commands to be interpreted before the rest of the %pre section. Identify the interpreter, such as `/usr/bin/python`, in the top field then include the commands to be intepreted below it, and click **Update Pre**.

#### *6.4.10.4.6. Kickstart Details ⇒ Post* —

Enables you to include the %post script and other parameters in the kickstart profile through the following subtabs:

#### *6.4.10.4.6.1. Kickstart Details ⇒ Post ⇒ Details —*

Allows editing of the %post script and inclusion of other options to be set after initial kickstart. You may alter individual commands within the script, identify the package profile to be used during synchronization, and include the activation key to be used for registration. If you plan to include multiple activation keys, first refer to Section 6.4.7.2 *Using Multiple Activation Keys at Once —* for an explanation of how conflicts are resolved.

In addition, you may predetermine whether configuration management and remote commands may be carried out on the system using the checkboxes at the bottom of the page. Make your changes and click the **Update Post** button.

#### *6.4.10.4.6.2. Kickstart Details ⇒ Post ⇒ GPG and SSL keys —*

Displays all of the GPG and SSL keys created by your organization. To include GPG and SSL keys you have created in the %post section, select the keys and click the **Update Keys** button. Refer to Section 6.4.10.8 *Kickstart ⇒ GPG and SSL Keys —* for instructions on creating keys.

**Caution**

When kickstarting systems receiving updates through either an RHN Proxy Server or RHN Satellite Server:, you must import that server's SSL certificate at the **Kickstart/GPG and SSL Keys** page and associate it with all relevant kickstart profiles. This association should be made on the **GPG and SSL keys** subtab of the **Kickstart Details** page. Not doing this will result in SSL_CERTIFICATE errors, and the kickstart will never report as complete in the RHN website.

#### *6.4.10.4.6.3. Kickstart Details ⇒ Post ⇒ --nochroot —*

Allows for the inclusion of commands to be executed before commands in the regular %post section and outside of the chroot. Refer to the *Red Hat Enterprise Linux System Administration Guide* for potential uses.

#### *6.4.10.4.6.4. Kickstart Details ⇒ Post ⇒ --interpreter —*

Like the same subtab under **Pre**, this enables you to specify an interpreter and specific commands to be interpreted before the rest of the %post section. Since the post script runs after the install, the full range of system commands is available, such as `/usr/bin/perl`. Identify the interpreter in the top field then include the commands to be intepreted under it, and click **Update Post**.

#### *6.4.10.4.7. Kickstart Details ⇒ IP Addresses —*

Identifies the IP address ranges to be presented with this kickstart profile upon request. Conflicts between IP address ranges will not be allowed unless one range is a subset of another, in which case the kickstart associated with the smallest of the enclosing ranges will be presented. Enter the range and click the **Update IP ranges** button. New fields will appear allowing you to enter additional ranges.

#### 6.4.10.5. Kickstart ⇒ Profiles —

Lists the kickstart profiles created by your organization. Click a name to see the **Kickstart Details** page. To enable inactive profiles, select the appropriate checkboxes and click the **Update Profiles**.

#### 6.4.10.6. Kickstart ⇒ IP Ranges —

Lists the IP addresses that have been associated with kickstart profiles created by your organization. Click either the range or the profile name to access different tabs of the **Kickstart Details** page.

#### 6.4.10.7. Kickstart ⇒ Sessions

Lists kickstart processes underway. Click the name of the system to obtain details about the kickstart session, including its progress, the action now taking place and the next to occur.

#### 6.4.10.8. Kickstart ⇒ GPG and SSL Keys —

Lists keys and certificates available for inclusion in kickstart profiles and provides a means to create new ones. This is especially important for customers of RHN Satellite Server or RHN Proxy Server because systems being kickstarted by them will need to have the server key imported into RHN and associated with the relevant kickstart profiles. Import it by creating a new key here and then make the profile association in the **GPG and SSL keys** subtab of the **Kickstart Details** page.

To develop a new key/certificate, click **create new cryptokey** in the upper-right corner of the page. Enter a description, select the type, upload the file, and click the **Update Key** button. Note that a unique description is required.

#### 6.4.10.9. Kickstart ⇒ Distributions —

Enables you to identify custom installation trees that may be used for kickstarting. (Satellite users should note that this does not display Red Hat distributions provided to them. They can be found within the **Distribution** dropdown menu of the **Kickstart Details** page.) Before creating a distribution, you will need to make an installation tree available, as described in the *Kickstart Installations* chapter of the *Red Hat Enterprise Linux 3 System Administration Guide*. This tree will need to be located in a public directory on an HTTP or FTP server.

**Important**

RHN Satellite Server users should note that channels imported with `satellite-sync` are made available automatically and do not require the creation of a separate installation tree. These trees are available to client systems that kickstart through the Satellite. While you may be able to access the files from a non-kickstarting client, this functionality is not supported and may be removed at any time in the future.

To create a new distribution, enter an intuitive label (without spaces) in the **Distribution Label** field, such as **`my-orgs-rhel-as-3`**. In the **External Location** field, paste the URL to the base of the installation tree. (You can test this by appending "README" to the URL in a Web browser, hitting return, and ensuring the distribution's readme file appears.)

In the **Autokickstart RPM** field, enter the auto-ks kernel image for the distribution. You can find all of the available packages by searching packages for "auto-kickstart". Identify the appropriate package

based upon the distribution to be kickstarted. It should look something like, "auto-kickstart-ks-rhel-i386-as-3". Then, strip everything preceding the "ks" to derive the boot image. For instance, in the above example, you would put "ks-rhel-i386-as-3" in the **Autokickstart RPM** field.

Then select the matching distribution from the **Base Channel** and **Installer Generation** dropdown menus, such as **Red Hat Enterprise Linux AS (v.3 for x86)** and **Red Hat Enterprise Linux 3**, respectively. When finished, click the **Create** button.

#### 6.4.10.10. Kickstart ⇒ File Preservation —

Collects lists of files to be protected and re-deployed on systems during kickstart. For instance, if you have many custom configuration files located on a system to be kickstarted, you can enter them here quickly as a list and then associate that list with the kickstart profile to be used.

To use this feature, click the **create new file preservation list** link at the top and enter a relevant label and all files and directories to preserved on the resulting page. Make sure you enter absolute paths to all files and directories. Then click **Create List**.

**Important**

Although file preservation is useful, it does have limitations. First, each list is limited to a total size of 1 MB. Further, special devices like `/dev/hda1` and `/dev/sda1` are not supported. Finally, only actual file and directory names may be entered. No regular-expression wildcards can be included.

When finished, you may include the file preservation list in the kickstart profile to be used on systems containing those files. Refer to Section 6.4.10.3 *Creating Kickstarts* for precise steps.

#### 6.4.10.11. Building Bootable Kickstart ISOs

While you can schedule a registered system to be kickstarted to a new operating system and package profile, it is also useful to be able to kickstart a system that is not registered with RHN, or does not yet have an operating system installed. One common method of doing this is to create a bootable CD-ROM that is inserted into the target system. When the system is rebooted, it boots from the CD-ROM, loads the kickstart configuration from the RHN Servers or your Satellite, and proceeds to install Red Hat Enterprise Linux according to the kickstart profile you have created.

To do this, copy the contents of `/isolinux` from the first CD-ROM of the target distribution. Then edit the `isolinux.cfg` file to default to 'ks'. Change the 'ks' section to look like this:

```
label ks
  kernel vmlinuz
  append text ks={url} initrd=initrd.img lang= devfs=nomount ramdisk_size=16438 \
  {ksdevice}
```

The URL can be obtained from the **Kickstart Details** page. It will look something like this:

```
http://my.sat.server/kickstart/ks/org/1271287x2c4682f33b87ed1d4dbea8/label/my-rhel3-as-ks
```

IP addressed-based kickstart URLs will look something like this:

```
http://my.sat.server/kickstart/ks/mode/ip_range
```

The kickstart distribution selected by the IP range should match the distribution you are building from, or errors will occur. {ksdevice} is optional, but looks like:

```
ksdevice=eth0
```

It is possible to change the distribution for a kickstart profile within a family, such as RHEL AS3 to RHEL ES3, by specifying the new distribution label. Note that you cannot move between versions (2.1 to 3) and between updates (U1 to U2).

Next, you may customize `isolinux.cfg` further for your needs, such as by adding multiple kickstart options, different boot messages, shorter timeout periods, etc.

Then make the ISO, as described in the *Making an Installation Boot CD-ROM* section of the *Red Hat Enterprise Linux 3 Installation Guide*. Or by issuing the command:

```
mkisofs -o file.iso -b isolinux.bin -c boot.cat -no-emul-boot -boot-load-size 4 \
-boot-info-table -R -J -v -T isolinux/
```

Note that `isolinux/` is the relative path to the directory containing the isolinux files you got from the distribution cd, while `file.iso` is the output iso file, put into the current directory.

You may then burn the ISO to CD-ROM. To use the disc (assuming you left the label for the kickstart boot as 'ks'), you should boot and type "ks" at the prompt. When you hit enter, the kickstart should begin.

#### 6.4.10.12. Integrating Kickstart with PXE

In addition to CD-ROM-based installs, RHN supports kickstarts through a Pre-Boot Execution Environment (PXE). This is less error prone than CDs, enables kickstarting from bare metal, and integrates with existing PXE/DHCP environments.

To use this method, you should make sure your systems have network interface cards (NIC) that support PXE, install and configure a PXE server, ensure DHCP is running, and then place the appropriate files on an HTTP server for deployment. Once the kickstart profile has been created, you may use the URL from the **Kickstart Details** page, just as you do for CD-ROM-based installs.

To obtain specific instructions for conducting PXE kickstarts, refer to the *PXE Network Installations* chapter of the *Red Hat Enterprise Linux 3 System Administration Guide*.

**Tip**

Upon running the **Network Booting Tool** as described in the Red Hat Enterprise Linux 3: System Administration Guide, ensure you select "HTTP" as the protocol and include the domain name of the RHN Satellite Server in the Server field if you intend to use it to distribute the installation files.

## 6.5. Errata

If you click the **Errata** tab on the top navigation bar, the **Errata** category and links appear. The pages in the **Errata** category allow you to track and manage Errata Updates.

**Tip**

If you want to receive an email when Errata Alerts are issued for your system, go to **Your RHN** => **Your Preferences** and select **Receive email notifications**.

Red Hat releases Errata Alerts in three categories, or types: Security Alerts, Bug Fix Alerts, and Enhancement Alerts. Each Errata Alert is comprised of a summary of the problem and the solution, including the RPM packages required to fix the problem.

Icons are used to identify the three types of Errata Alerts:

- — Security Updates available, update *strongly* recommended
- — Bug Fix Updates available and recommended
- — Enhancement Updates available

In addition to the pages described within this chapter, you may view Errata by product line from the following location: https://rhn.redhat.com/errata.

### 6.5.1. Relevant Errata

As shown in Figure 6-5, the **Relevant Errata** page displays a customized list of Errata Alerts that applies to your registered systems. The list provides a summary of each Errata Alert, including its type, advisory, synopsis, systems affected, and date updated.

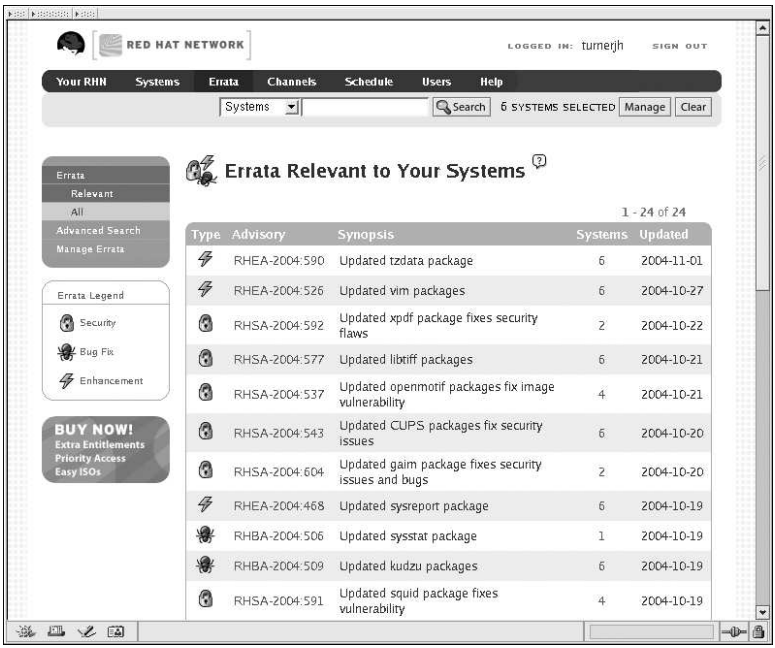


**Figure 6-5. Errata List**

Clicking on the Advisory takes you to the **Details** tab of the **Errata Details** page. Clicking on the number of associated systems takes you to the **Affected Systems** tab of the **Errata Details** page. Refer to Section 6.5.2.2 *Errata Details* for more information.

### 6.5.2. All Errata

The **All Errata** page displays a list of all Errata Alerts released by Red Hat. It works much the same as the **Relevant Errata** page in that clicking either the Advisory or the number of systems affected takes you to related tabs of the **Errata Details** page. Refer to Section 6.5.2.2 *Errata Details* for more information.

#### 6.5.2.1. Apply Errata Updates

Errata Alerts include a list of updated packages that are required to apply the Errata Update. To apply Errata Updates to a system, the system must be entitled.

You can apply all applicable Errata Updates to a system by clicking on **Systems => Systems** in the top and left navigation bars. Click on the name of an entitled system, and click the **Errata** tab of the resulting **System Details** page. When the Relevant Errata list appears, click **Select All** then the **Apply Errata** button on the bottom right-hand corner of the page. Only those Errata that have not been scheduled or were scheduled and failed or canceled are listed. Updates already pending are excluded from the list.

In addition, Management and Provisioning users can apply Errata Updates using two other methods:

- To apply a specific Errata Update to one or more systems, find the update within the Errata lists or by searching. In the table, click on the number of systems affected, which will take you to the **Affected Systems** tab of the **Errata Details** page. Then, individually select the systems to be updated and click the **Apply Errata** button. Double-check the systems to be updated on the confirmation page, then click the **Confirm** button.
- To apply more than one Errata Update to one or more systems, select the systems from a **Systems** list and click the **Update List** button. Click the **System Set Manager** link in the left navigation bar, then click the **Systems** tab. After ensuring the appropriate systems are selected, click the **Errata** tab, select the Errata Updates to apply, and click the **Apply Errata** button. You can select to apply the Errata as soon as possible (the next time the Red Hat Network Daemon on the client systems connect to RHN) or schedule a date and time for the Errata Updates to occur. Then click the **Schedule Updates** button. You can follow the progress of the Errata Updates through the **Pending Actions** list. Refer to Section 6.7 *Schedule* for more details.

**Important**

If you use scheduled package installation, the packages will be installed via the RHN Daemon. You must have the RHN Daemon enabled on your systems. Refer to Chapter 3 *Red Hat Network Daemon* for more details.

The following rules apply to Errata Updates:

- Each package is a member of one or more channels. If a selected system is not subscribed to a channel containing the package, the package will not be installed on that system.
- If a newer version of the package is already on the system, the package will not be installed on that system.
- If an older version of the package is installed, the package will be upgraded.

#### 6.5.2.2. Errata Details

If you click on the Advisory of an Errata Alert in the **Relevant** or **All** pages, its **Errata Details** page appears. This page is further divided into the following tabs:

##### *6.5.2.2.1. Errata Details ⇒ Details*

Provides the Errata Report issued by Red Hat. It describes the problem and solution and lists the channels it affects. Clicking on a channel name displays the **Packages** tab of the **Channel Details** page. Refer to Section 6.6.1.4 *Software Channel Details* for more information.

##### *6.5.2.2.2. Errata Details ⇒ Packages*

Provides links to each of the updated RPMs broken down by channel. Clicking on the name of a package displays its **Package Details** page. Refer to Section 6.6.5.3 *Package Details* for more information.

##### *6.5.2.2.3. Errata Details ⇒ Affected Systems*

Lists systems affected by the Errata Alert. You can apply updates here. (See Section 6.5.2.1 *Apply Errata Updates*.) Clicking on the name of a system takes you to its **System Details** page. Refer to Section 6.4.2.6 *System Details* for more information.

To help users determine whether an update has been scheduled, a Status column exists within the affected systems table. Possible values are: None, Pending, Picked Up, Completed, and Failed. This column identifies only the latest action related to an Errata. For instance, if an action fails and you reschedule it, this column will show the status of the Errata as Pending only (with no mention of the previous failure). Clicking a status other than None takes you to the **Action Details** page. This column corresponds to one on the **Errata** tab of the **System Details** page.

### 6.5.3. Advanced Search

The **Advanced Search** page allows you to search through Errata according to specific criteria, such as summary, advisory, and package name. Type your keyword, select the criterion to search by, and click the **Search** button. The results appear at the bottom of the page.

## 6.6. Channels

If you click the **Channels** tab on the top navigation bar, the **Channels** category and links appear. The pages in the **Channels** category enable you to view and manage the channels and packages associated with your systems. In addition, you can obtain ISO images here.

### 6.6.1. Software Channels

The **Software Channels** page is the first to appear in the **Channels** category. A software channel is a list of Red Hat Enterprise Linux packages grouped by use. Channels are used to choose packages to be installed on a system.

There are two types of software channels: *base channels* and *child channels*. A base channel consists of a list of packages based on a specific architecture and Red Hat Enterprise Linux release. For example, all the packages in Red Hat Enterprise Linux 2.1 for the x86 architecture make up a base channel. The list of packages in Red Hat Enterprise Linux 2.1 for the Itanium architecture make up a

different base channel. A child channel is a channel associated with a base channel but contains extra packages. For instance, an organization can create a child channel associated with Red Hat Enterprise Linux 2.1 for the x86 architecture that contains extra packages needed only for the organization, such as a custom engineering application.

A system must be subscribed to one base channel only. This base channel is assigned automatically during registration based upon the Red Hat Enterprise Linux release and system architecture selected. In the case of public free channels, the action will succeed. In the case of paid base channels, this action will fail if an associated entitlement doesn't exist.

A system can be subscribed to multiple child channels of its base channel. Only packages included in a system's subscribed channels can be installed or updated on that system. Further, RHN Satellite Server and RHN Proxy Server customers have channel management authority. This authority gives them the ability to create and manage their own custom channels. Refer to the *RHN Channel Management Guide* for details.

Channels can be further broken down by their relevance to your systems. Two such lists emerge: **Relevant** and **All**.

#### 6.6.1.1. Relevant Channels

As shown in Figure 6-6, the **Relevant Channels** page is shown by default when you click **Software Channels** in the left navigation bar. It displays a list of channels now associated with your systems. Links within this list go to different tabs of the **Software Channel Details** page. Clicking on a channel name takes you to the **Details** tab. Clicking on the packages number takes you to the **Packages** tab. And clicking on the systems number takes you to the **Subscribed Systems** tab. Refer to Section 6.6.1.4 *Software Channel Details* for details.

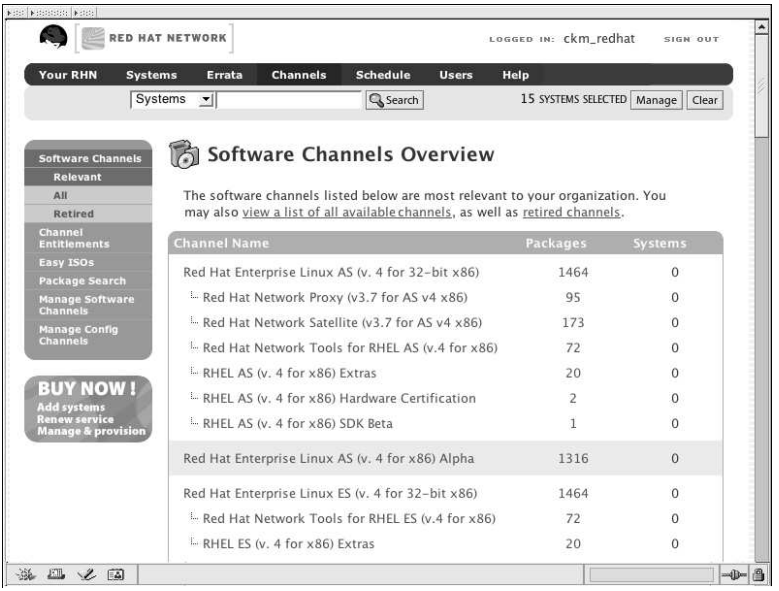
RED HAT NETWORK
LOGGED IN: ckm_redhat
SIGN OUT
Your RHN
Systems
Errata
Channels
Schedule
Users
Help
Systems
Search
15 SYSTEMS SELECTED
Manage
Clear
Software Channels
Relevant
All
Retired
Channel Entitlements
Easy ISOs
Package Search
Manage Software Channels
Manage Config Channels
BUY NOW !
Add systems
Renew service
Manage & provision
Software Channels Overview
The software channels listed below are most relevant to your organization. You may also view a list of all available channels, as well as retired channels.
Channel Name
Packages
Systems
Red Hat Enterprise Linux AS (v. 4 for 32-bit x86) 1464 0
Red Hat Network Proxy (v3.7 for AS v4 x86) 95 0
Red Hat Network Satellite (v3.7 for AS v4 x86) 173 0
Red Hat Network Tools for RHEL AS (v.4 for x86) 72 0
RHEL AS (v. 4 for x86) Extras 20 0
RHEL AS (v. 4 for x86) Hardware Certification 2 0
RHEL AS (v. 4 for x86) SDK Beta 1 0
Red Hat Enterprise Linux AS (v. 4 for x86) Alpha 1316 0
Red Hat Enterprise Linux ES (v. 4 for 32-bit x86) 1464 0
Red Hat Network Tools for RHEL ES (v.4 for x86) 72 0
RHEL ES (v. 4 for x86) Extras 20 0

**Figure 6-6. Relevant Channels**

#### 6.6.1.2. Retired Channels

The **Retired Channels** page displays channels available to your organization that have reached their end-of-life dates. These channels do not receive updates.

#### 6.6.1.3. All Channels

The **All Channels** page can be retrieved by clicking **All** below **Software Channels** in the left navigation bar. It works identically to the **Relevant** button with one exception; It displays all software channels offered by Red Hat Network, regardless of whether you have systems associated with them.

#### 6.6.1.4. Software Channel Details

If you click on the name of a channel, the **Software Channel Details** page will appear. This page is broken down into the following tabs:

##### *6.6.1.4.1. Software Channel Details ⇒ Details*

General information about the channel and the parent channel, if it is a child channel. This is the first tab you see when you click on a channel. It displays essential information about the channel, such as summary, description, and architecture.

— In addition, a Globally Subscribable checkbox can be seen by Organization Administrators and Channel Administrators. This signifies the default behavior of every channel allowing any user to subscribe systems to it. Unchecking this box and clicking **Update** causes the appearance of a **Subscribers** tab, which may then be used to grant certain users subscription permissions to the channel. Organization Administrators and Channel Administrators can always subscribe systems to any channel.

— Only customers with custom base channels may change their systems' base channel assignment. They may do this through the website in two ways:

- The customer has its own base channel and it is assigning the system to that new base channel.
- The customer has its own base channel and, having assigned a system to this base channel, it subsequently reverts the system to its original distribution-based base channel.

##### *6.6.1.4.2. Software Channel Details ⇒ Subscribers —*

List of users who have subscription permissions to the channel. This tab appears on two conditions: First, the logged in user must be an Organization Administrator or a Channel Administrator. Second, the Globally Subscribable checkbox on the **Details** tab must be unchecked, thereby making the channel subscribable by user. On this tab, select the checkboxes of the users to be allowed to subscribe systems to this channel and click **Update**. Note that Organization Administrators and Channel Administrators automatically have subscription access to all channels.

##### *6.6.1.4.3. Software Channel Details ⇒ Managers —*

List of users who have permission to manage the channel. This tab is applicable only to RHN Proxy Server and RHN Satellite Server customers with custom channel management privileges. It works much like the **Subscribers** tab but is available only for channels owned by the organization. There is no Globally Managable flag like there is for subscription. Being checked in the **Managers** tab for a

channel means that a user is a Channel Administrator but only for that channel. He cannot create new channels or clone them.

#### *6.6.1.4.4. Software Channel Details ⇒ Errata*

List of Errata affecting the channel. The list displays advisory types, names, summaries, and the dates issued. Clicking on an advisory name takes you to its **Errata Details** page. Refer to Section 6.5.2.2 *Errata Details* for more information.

#### *6.6.1.4.5. Software Channel Details ⇒ Packages*

List of packages in the channel. To download packages as a .tar file, select them and click the **Download Packages** button at the bottom-left corner of the page. Clicking on a package name takes you to the **Package Details** page. This page displays a set of tabs with information about the package, including which architectures it runs on, the package size, build date, package dependencies, the change log, list of files in the package, newer versions, and which systems have the package installed. From here, you can download the packages as RPMs or SRPMs. Refer to Section 6.6.5.3 *Package Details* for more information.

If you are looking for a specific package or a subset of packages, you can use the package filter on the top of the list. Entering a substring to search for will search all the packages in the list for the substring at the beginning, in the middle, or at the end of the package name. For example, typing **`ks`** in the filter might return all the `ksconfig`, `krb5-workstation`, and `links`. The filter is case-insensitive.

#### *6.6.1.4.6. Software Channel Details ⇒ Subscribed Systems*

List of entitled systems subscribed to the channel. The list displays system names, base channels, and their levels of entitlement. Clicking on a system name takes you to its **System Details** page. Refer to Section 6.4.2.6 *System Details* for more information.

— If it is a child channel, you will also have the option within this tab of unsubscribing systems from the channel. Use the checkboxes to select the systems, then click the **Unsubscribe** button on the bottom right-hand corner.

#### *6.6.1.4.7. Software Channel Details ⇒ Target Systems*

List of entitled systems that are eligible to be subscribed to the channel. This tab appears only for child channels. Use the checkboxes to select the systems, then click the **Subscribe** button on the bottom right-hand corner. You will receive a success message or be notified of any errors. This can also be accomplished through the **Channels** tab of the **System Details** page. Refer to Section 6.4.2.6 *System Details* for more information.

#### *6.6.1.4.8. Software Channel Details ⇒ Downloads*

ISO images associated with the channel. This tab appears only for base channels. Links on the **Easy ISOs** pages bring you to this tab for the related channel. Red Hat recommends using **curl** or **wget** for ISO downloads. Click the **help on using curl or wget** link for precise instructions.

#### *6.6.1.4.9. Software Channel Details ⇒ License*

Text of the channel's End User License Agreement. This tab is associated only with channels of third-party providers. It appears when you attempt a subscription to such a channel through the **Target**

**Systems** tab. To complete the subscription, read the agreement, click the **Accept** button, and then click the **Confirm** button. To decline the subscription, click the **Cancel** button.

### 6.6.2. Channel Entitlements

The **Channel Entitlements** page displays the list of channels for which you have paid. Click the number of systems subscribed to see a list of systems tied to the corresponding channel.

### 6.6.3. Easy ISOs

The **Easy ISOs** pages provide direct access to the ISO images available to you. These images, comprising full installations of various Red Hat operating system distributions, are actually located within the **Downloads** tab of the **Channel Details** page. This feature is available only to paid RHN subscribers.

To download an ISO image, Red Hat recommends copying its URL and using either **curl** or **wget**. Click the **help on using curl or wget** link for precise instructions. To obtain the URL, right-click on the disc link and select to open the link in a new window or tab. You may then cancel the download, copy the lengthy URL from the location bar, and paste it into the **curl** or **wget** command.

Once downloaded, either burn the images to CD-Rs or CD-RWs or copy them to the machine for direct installation. Refer to http://www.redhat.com/download/howto_download.html for additional download instructions and steps to burn images to discs. Refer to the operating system's respective installation guide for instructions on installing from CD-ROM or hard drive, available at http://www.redhat.com/docs/.

ISOs can be further broken down by their relevance to your systems. Two such lists emerge: **Relevant** and **All**.

#### 6.6.3.1. Relevant ISOs

The **Relevant ISOs** page is shown by default when you click **Easy ISOs** in the left navigation bar. It displays a list of ISOs by channel now associated with your systems. Links within this list go to the **Downloads** tab of the **Channel Details** page. Refer to Section 6.6.3 *Easy ISOs* for instructions on use.

#### 6.6.3.2. All ISOs

The **All ISOs** page can be retrieved by clicking **All** below **Easy ISOs** in the left navigation bar. It works identically to the **Relevant** button with one exception; It displays all ISOs available to you through Red Hat Network, regardless of whether you have systems associated with the related channels. Refer to Section 6.6.3 *Easy ISOs* for instructions on use.

### 6.6.4. Package Search

The **Package Search** page allows you to search through packages using various criteria. You may search by name or name and summary, within relevant or all channels, or within specific architectures. Type your keyword, select the criterion to search by, and click the **Search** button. The results appear at the bottom of the page.

### 6.6.5. Software Packages

A software package is the smallest essential ingredient of any Red Hat Enterprise Linux system. Packages, commonly known as RPMs because of their oversight by RPM Package Manager, are the pieces of software that, when installed, enable your system to operate. Packages are grouped by channels to help you more easily determine which are applicable to your systems.

These packages can be retrieved in one of two ways: by direct install or through download.

#### 6.6.5.1. Software Package Install

Only software packages included in a system's subscribed channels can be installed or updated on that system.

To apply Errata Updates, refer to Section 6.5.2.1 *Apply Errata Updates*. To upgrade and install packages through the **Systems** category, use the **Packages** tab of the **System Details** page. Refer to Section 6.4.2.6 *System Details* for instructions.

— Within the **Channels** category, you may install an individual package on multiple entitled systems by following these steps:

1. Select **Channels** => **Software Channels** from the top and left navigation bars.
2. Click on the name of the channel that contains the package to be installed.
3. On the **Software Channel Details** page, click on the **Packages** tab.
4. Click on the name of the package you want to install.
5. On the **Package Details** page, click on the **Target Systems** tab.
6. Select the entitled systems you want to install the package on.
7. Click on the **Install Packages** button.
8. Confirm the action.
9. The action is added to the **Pending Actions** list under the **Schedule** tab in the top navigation bar.

#### 6.6.5.2. Package Download

If you do not want to schedule a package installation, you can download the packages immediately. If you download the packages, you must install them manually.

To download packages through the **Systems** category, refer to Section 6.4.2.6 *System Details*.

To download individual RPMs and SRPMs through the **Channels** category, follow these steps:

1. Select **Channels** => **Software Channels** from the top and left navigation bars.
2. Click on the name of the channel that contains the package to be downloaded.
3. On the **Software Channel Details** page, click on the **Packages** tab.
4. Click on the name of the package that you want to download.
5. On the **Package Details** page, click the **Download RPM** or **Download SRPM** link on the bottom right-hand corner.
6. Confirm the action.

The next step is to install the packages manually. Refer to Section 2.3.5.2 *Manual Package Installation* for details.

#### 6.6.5.3. Package Details

If you click on the name of any package in the website, the **Package Details** page will appear. This page contains the following tabs:

##### *6.6.5.3.1. Package Details ⇒ Details*

Details about the package, including subtabs for overview, dependencies, change log, and file list:

###### *6.6.5.3.1.1. Package Details ⇒ Details ⇒ Overview*

A summary of the package, including the package description, size, and version. (This information is similar to issuing the command `rpm -qi packagename` but with more detail.) Click the links in the bottom right-hand corner of the page to download the RPM and/or SRPM files for the package.

###### *6.6.5.3.1.2. Package Details ⇒ Details ⇒ Dependencies*

A list of all other packages that must also be installed on the system for this one to function properly. It also lists packages that it obsoletes or has conflicts with.

###### *6.6.5.3.1.3. Package Details ⇒ Details ⇒ Change Log*

The events of this package's history listed in reverse chronological order. (This information is similar to issuing the command `rpm -q --changelog packagename`.)

###### *6.6.5.3.1.4. Package Details ⇒ Details ⇒ File List*

A list of the files that comprise this package, including their MD5 Sums and sizes. (This information is similar to issuing the command `rpm -ql packagename`.)

##### *6.6.5.3.2. Package Details ⇒ Newer Versions*

List of newer versions of the packages released via Errata Alerts.

##### *6.6.5.3.3. Package Details ⇒ Installed Systems*

List of systems with this package installed.

##### *6.6.5.3.4. Package Details ⇒ Target Systems —*

List of systems on which the package can be installed. Go here to install packages on entitled systems. Refer to Section 6.6.5.1 *Software Package Install* for instructions.

## 6.6.6. Manage Config Channels —

Provides the means to create and oversee channels containing configuration files. You must be an Configuration Administrator or Organization Administrator to view this section of the website. Like software channels, configuration channels store files to be installed on systems. Unlike software packages, various versions of configuration files may prove useful to a system at any given time. Further, RHN allows you to include variables, or macros, that may make your configuration files templates that can be deployed across your organization, with the relevant values populated upon individual system installation.

Please note that whenever a configuration file is deployed via RHN, a backup of the previous file including its full path is made in the `/var/lib/rhncfg/backups/` directory on the affected system. The backup will retain its filename but have a `.rhn-cfg-backup` extension appended.

### 6.6.6.1. Preparing Systems for Config Management

For a system to have its configuration managed through RHN, it must have the appropriate tools and config-enable file installed. These tools may already be installed on your system, especially if you kickstarted the system with configuration management functionality. If not, they can be found within the RHN Tools child channel for your distribution. Download and install the latest `rhncfg*` packages. They are:

- `rhncfg` — The base libraries and functions needed by all `rhncfg-*` packages.
- `rhncfg-actions` — The code required to run configuration actions scheduled via the RHN website.
- `rhncfg-client` — A command line interface to the client features of the RHN Configuration Management system.
- `rhncfg-management` — A command line interface used to manage RHN configuration.

Next, you must place a config-enable file on the system to have config actions scheduled. This file is required to allow configuration management on the system while preventing inadvertent and potentially dangerous changes. To create this file, issue the following commands as root on the target system. First, create the necessary directory:

```
mkdir -p /etc/sysconfig/rhn/allowed-actions/configfiles
```

Then, you should decide exactly what actions should be allowed by system administrators. The following modes are available:

- **deploy** — Install configuration files from the central repository on the system. Without this set, the configuration management interface provides no real value for this system.
- **verify** — Identify any differences between configuration files on the system and those associated with it in the central repository.
- **diff** — Display differences between configuration files on the system and those associated with it in the central repository.
- **upload** — Send any files from the system to the central repository. This is similar to granting root privileges on the machine.
- **mtime_upload** — Send files modified since a certain date and time from the system to the central repository.
- **all** — Enable all of these modes for configuration management on the system.

To set individual modes, issue this command (repeatedly, as root), appending the mode name to the end:

```
touch /etc/sysconfig/rhn/allowed-actions/configfiles/mode
```

To grant full configuration management access, issue this command:

```
touch /etc/sysconfig/rhn/allowed-actions/configfiles/all
```

Your system should now be ready for config management through RHN. Command line options also exist for many of these functions. Refer to Appendix A *Command Line Config Management Tools* for instructions.

#### 6.6.6.2. Manage Config Channels ⇒ Config Channels —

There are two types of configuration channels: *global channels* and *system-specific channels*. A global channel contains configuration files developed across your organization. These may well be applicable to multiple systems. A system-specific channel consists of local override configuration files tied to particular systems. These files take precedent over all other configurations.

##### *6.6.6.2.1. Manage Config Channels ⇒ Config Channels ⇒ Global —*

Shown by default when you click **Manage Config Channels** in the left navigation bar, the **Global Config Channels** displays a list of configuration channels managed by your organization. Links within this list go to different tabs of the **Configuration Channel Details** page. Clicking on a channel name takes you to the **Details** tab. Clicking on the files number takes you to the **Files** tab. And clicking on the systems number takes you to the **Systems** tab. Refer to Section 6.6.6.5 *Configuration Channel Details —* for instructions.

##### *6.6.6.2.2. Manage Config Channels ⇒ Config Channels ⇒ System —*

The **System Config Channels** page can be retrieved by selecting it from the pulldown menu on the main **Manage Config Channels** page. It displays local override (system-specific) configuration channels and works similarly to the **Global Config Channels** page in that clicking the name of a system takes you to the **List** subtab of the **Configuration Channel Details** page. Refer to Section 6.6.6.5 *Configuration Channel Details —* for instructions.

#### 6.6.6.3. Manage Config Channels ⇒ Manage Files —

The **Manage Files** page lists the configuration files managed by your organization. The files here are listed by path. A given path can exist in many configuration channels, but each instance of a path in each configuration channel is treated as a seperate entity.

Clicking the number in the Config Channels column takes you to a list of channels containing the file. From there you can access tabs of the **Configuration Channel Details** page. Clicking the number in the Latest Revision column takes you to the **Configuration File Details** page. Refer to Section 6.6.6.6 *Configuration File Details —* for instructions.

#### 6.6.6.4. Manage Config Channels ⇒ Quota —

The **Quota** page displays the amount of disk space alloted and used for storing configuration files. A summary of available and used space can be found at the top, while individual file use is listed within the table. Click the filename to go to the **Configuration File Details** page. Refer to Section

6.6.6.6 *Configuration File Details* — for instructions. Click the config channel name to access the **Configuration Channel Details** page. Refer to Section 6.6.6.5 *Configuration Channel Details* — for instructions.

### 6.6.6.5. Configuration Channel Details —

If you click on the name of a channel in a list, the **Configuration Channel Details** page will appear. This page contains the following tabs:

#### *6.6.6.5.1. Configuration Channel Details ⇒ Details* —

General information about the channel. This is the first tab you see when you click on a channel. It displays basic information about the channel, including name and description, and provides the means to alter this information. To make changes, enter new values in the text fields and click the **Edit Config Channel** button.

#### *6.6.6.5.2. Configuration Channel Details ⇒ Files* —

Configuration files associated with this channel. Use the subtabs to view, upload, and create files.

#### *6.6.6.5.2.1. Configuration Channel Details ⇒ Files ⇒ List* —

Displays the files and directories associated with the configuration channel. Files are represented by a *paper* icon while directories display *folder* icons. Click the name of a file or directory to go to its details page. Refer to Section 6.6.6.6 *Configuration File Details* — for instructions. To replicate a file within a config channel, select its checkbox, click the **Copy to Config Channel** button, and select the destination channel. To remove a file, select it and click **Delete Selected Files**.

#### *6.6.6.5.2.2. Configuration Channel Details ⇒ Files ⇒ Upload* —

Enables you to import files from your system into RHN's central configuration manager. The Deploy File Path is the path to which the file will be deployed on a target system, and Local File is the file you want to upload from your system to RHN.

To do this, populate all fields, browse for the file, and click the **Upload File** button. Note that files larger than 16 KB cannot be edited through the RHN website. The file path is the location to which the file will be deployed. The user, group, and mode fields allow you to set the file's ownership and permissions.

#### *6.6.6.5.2.3. Configuration Channel Details ⇒ Files ⇒ Create File* —

Allows you to create a configuration file from scratch within the interface. The fields here work similarly to those on the **Upload** subtab: Path is the location to which the file will be deployed. The user, group, and mode fields allow you to set the file's ownership and permissions. Include the actual file in the contents field. When finished, click the **Create Config File** button.

#### *6.6.6.5.2.4. Configuration Channel Details ⇒ Files ⇒ Create Directory —*

Allows you to create a configuration directory within the interface. The fields resemble those on the **Upload** and **Create File** subtab: Path is the absolute location of the directory on the system. The user, group, and mode fields allow you to set the directory's ownership and permissions. When finished, click the **Create Config Directory** button.

#### *6.6.6.5.3. Configuration Channel Details ⇒ Systems —*

Identifies the systems subscribed to this configuration channel. Clicking a system name takes you to the **System Details** page.

#### *6.6.6.5.4. Configuration Channel Details ⇒ Target Systems —*

Displays all of the systems that have Provisioning entitlements but are not yet subscribed to this config channel. To associate systems with the config channel, select their checkboxes and click the button matching the rank to be assigned. **Subscribe with Highest Rank** will override all other config channels, except local configs. **Subscribe with Lowest Rank** will rank this config channel below all others. When done, the selected systems will appear in the **Systems** tab.

### 6.6.6.6. Configuration File Details —

If you click on the name or number of a file in a list, the **Configuration File Details** page will appear. You may remove the file at anytime by clicking **delete file** in the upper-right corner of the page. This page contains the following tabs:

#### *6.6.6.6.1. Configuration File Details ⇒ Details —*

General information about the file. This is the first tab you see when you click on a file. It displays basic information about the file, including path, associated channel, revision, and date. It also provides links to download, view and edit the file, as well as identify whether it is binary. Note that files larger than 16 KB cannot be edited through the RHN website. In addition, you can define macros (variables) here that will have different values interpolated when installed on various systems. Refer to Section 6.6.6.7 *Including Macros in your Configuration Files* for a full description of this feature.

#### *6.6.6.6.2. Configuration File Details ⇒ Revisions —*

A list of the revisions of this configuration file in the current config channel. Every change to a configuration file creates a new revision of that file in the given config channel. The latest revision of a configuration file is always the only one provided by that channel. Revision numbers for a file are tied to a channel. So revision 3 of `/etc/foo` in config channel 'bar' is completely independent of revision 3 of `/etc/foo` in config channel 'baz'. You can examine revisions in the list or use the **Browse** and **Upload File** buttons to upload a more recent revision.

#### *6.6.6.6.3. Configuration File Details ⇒ Diff —*

A list of configuration files available for comparison. Click the name of the channel containing the file, then the name of the file itself. A list of differences will appear.

#### *6.6.6.6.4. Configuration File Details ⇒ Copy —*

A list of configuration channels that may receive a copy of the file. To copy the file to a channel, select the channel's checkbox, and click the **Copy File** button.

- **Copy to Config Channel** — Displays the global config channels for your organization. To copy the latest revision of this file to channels, select the appropriate checkboxes, and click the **Copy File** button.
- **Copy to System** — Displays the system-specific config channels for your organization. To copy the latest revision of this file to channels, select the appropriate checkboxes, and click the **Copy File** button.

### 6.6.6.7. Including Macros in your Configuration Files

Being able to store and share identical configurations is useful, but what if you have many variations of the same configuration file? What do you do if you have configuration files that differ only in system-specific details, such as hostname and MAC address?

In traditional file management, you would be required to upload and distribute each file separately, even if the distinction is nominal and the number of variations is in the hundreds or thousands. RHN addresses this by allowing the inclusion of macros, or variables, within the configuration files it manages for Provisioning-entitled systems. In addition to variables for custom system information, the following standard macros are supported:

- rhn.system.sid
- rhn.system.profile_name
- rhn.system.description
- rhn.system.hostname
- rhn.system.ip_address
- rhn.system.custom_info(key_name)
- rhn.system.net_interface.ip_address(eth_device)
- rhn.system.net_interface.netmask(eth_device)
- rhn.system.net_interface.broadcast(eth_device)
- rhn.system.net_interface.hardware_address(eth_device)
- rhn.system.net_interface.driver_module(eth_device)

To use this powerful feature, either upload or create a configuration file through the **Configuration Channel Details** page. Then, open its **Configuration File Details** page and include the supported macros of your choosing. Ensure the delimiters used to offset your variables match those set in the **Macro Start Delimiter** and **Macro End Delimiter** fields and do not conflict with other characters in the file. The delimiters must be two characters and cannot contain the percent (%) symbol.

As an example, you may have a file applicable to all of your servers that differs only in IP address and hostname. Rather than manage a separate configuration file for each server, you may create a single file, say `server.conf`, with the IP address and hostname macros included, like so:

```
hostname={@ rhn.system.hostname @}
ip_address={@ rhn.system.net_interface.ip_address(eth0) @}
```

Upon delivery of the file to individual systems, whether through a scheduled action in the RHN website or at the command line with the **Red Hat Network Configuration Client** (`rhncfg-client`),

the variables will be substituted with the actual hostname and IP address of the system, as recorded in RHN's System Profile, such as:

```
hostname=test.example.domain.com
ip_address=177.18.54.7
```

To capture custom system information, insert the key label into the custom information macro (rhn.system.custom_info). For instance, if you developed a key labeled "asset" you can add it to the custom information macro in a configuration file to have the value substituted on any system containing it. The macro would look like this:

```
asset={@ rhn.system.custom_info(asset) @}
```

Upon deployment of the file to a system containing a value for that key, the macro gets translated, such as:

```
asset=Example#456
```

To include a default value, for instance if one is required to prevent errors, you can append it to the custom information macro, like so:

```
asset={@ rhn.system.custom_info(asset) = 'Asset #' @}
```

This default will be overridden by the actual value on any system containing it. For instructions on developing custom system information keys, refer to Section 6.4.9 *Custom System Info* — .

Using the **Red Hat Network Configuration Manager** (`rhncfg-manager`) will not translate or alter files, as that tool is system agnostic. Binary files cannot be interpolated.

## 6.7. Schedule

If you click the **Schedule** tab on the top navigation bar, the **Schedule** category and links appear. These pages enable you to keep track of the actions taking place within your systems. An action is a scheduled RHN task that is to be performed on one or more client systems. For example, an action can be scheduled to apply all Errata Updates to a system.

Red Hat Network keeps track of the following action types:

1. Package Alteration (installation, upgrade, and removal)
2. Rollback Package Actions
3. System Reboots
4. Errata Updates
5. Configuration File Alteration (deploy, upload, and diff)
6. Hardware Profile Updates
7. Package List Profile Updates
8. Kickstart Initiation
9. Remote Commands

Each page in the **Schedule** category represents an action status.

### 6.7.1. Pending Actions

As shown in Figure 6-7, the **Pending Actions** page is shown by default when you click **Schedule** in the top navigation bar. It displays actions that have not started or are in progress.

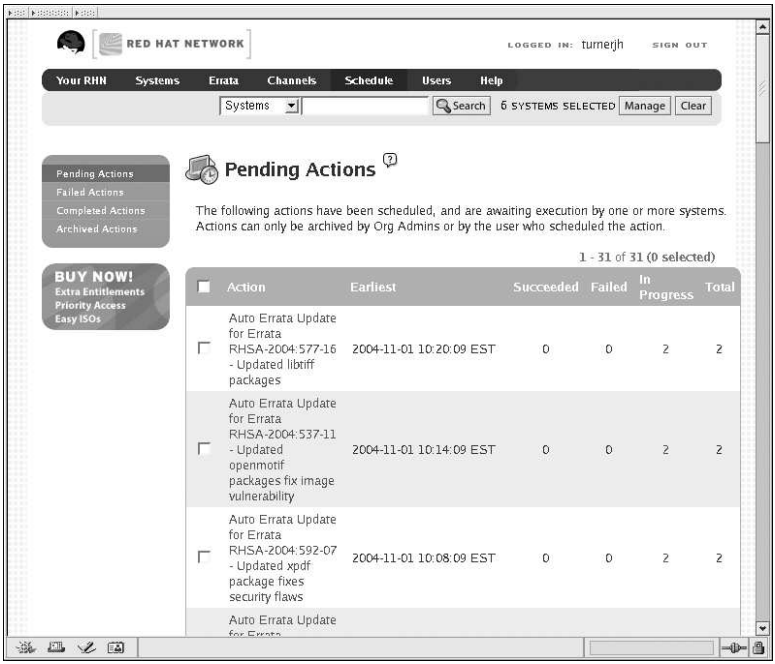


**Figure 6-7. Schedule - Pending Actions**

### 6.7.2. Failed Actions

Actions that could not be completed. If the action returns an error, it will be displayed.

### 6.7.3. Completed Actions

Actions that have succeeded.

### 6.7.4. Archived Actions

Actions that you have selected to store for review.

### 6.7.5. Actions List

In each page, each row in the list represents a single scheduled event or action that might affect multiple systems and involve various packages. The list contains several columns of information:

- **Select** — Use the checkboxes in this column to select actions. After selecting actions, you can either add them to your selection list or move them to the **Archived Actions** list. If you archive a pending action, it is not canceled; The action item just moves from the **Pending Actions** list to the **Archived Actions** list.
- **Action** — Type of action to perform such as Errata Update or Package Install. Clicking an action name takes you to its **Action Details** page. Refer to Section 6.7.5.1 *Action Details* for more information.
- **Earliest** — The earliest day and time the action will be performed.
- **Succeeded** — Number of systems on which this action was successful.
- **Failed** — Number of systems on which this action has been tried and failed.
- **In Progress** — Number of systems on which this action is taking place.
- **Total** — Total number of systems on which this action has been scheduled.

#### 6.7.5.1. Action Details

If you click on the name of an action, the **Action Details** page appears. This page is broken down into the following tabs:

##### *6.7.5.1.1. Action Details ⇒ Details*

General information about the action. This is the first tab you see when you click on an action. It displays the action type, scheduling administrator, earliest execution, and notes. Clicking the Errata Advisory takes you to the **Errata Details** page.The Errata Advisory appears only if the action is an Errata Update. Refer to Section 6.5.2.2 *Errata Details* for more information.

##### *6.7.5.1.2. Action Details ⇒ Completed Systems*

List of systems on which the action has been successfully undertaken. Clicking a system name takes you to its **System Details** page. Refer to Section 6.4.2.6 *System Details* for more information.

##### *6.7.5.1.3. Action Details ⇒ In Progress Systems*

List of systems on which the action is now being undertaken. To cancel an action, select the system using the appropriate checkbox and click the **Unschedule Action** button. Clicking a system name takes you to its **System Details** page. Refer to Section 6.4.2.6 *System Details* for more information.

##### *6.7.5.1.4. Action Details ⇒ Failed Systems*

List of systems on which the action has been attempted and failed. The actions can be rescheduled here. Clicking a system name takes you to its **System Details** page. Refer to Section 6.4.2.6 *System Details* for more information.

## 6.8. Users —

Only Organization Administrators can see the **Users** tab on the top navigation bar. If you click the **Users** tab, the **Users** category and links appear. These pages enable you to grant and edit permissions

for those who will administer your system groups. Click in the **User List** to modify users within your organization.

### 6.8.1. User Roles

To delegate responsibilities within your organization, Red Hat Network provides several roles with varying degrees of responsibility and access. This list describes the permissions of each and the differences between them:

- **User** — Also known as a *System Group User*, this is the standard role associated with any newly created user. This person may be granted access to manage system groups and software channels. The systems must be in system groups to which the user has permissions for them to be manageable or even visible. Remember, however, all globally subscribable channels may be used by anyone.
- **Activation Key Administrator** — This role is designed to manage your organization's collection of activation keys. This person can create, modify, and delete any key within your overarching account.
- **Software Channel Administrator** — This role has complete access to the software channels and related associations within your organization. It requires RHN Satellite Server or RHN Proxy Server. This person may change the base channels of systems, make channels globally subscribable, and create entirely new channels.
- **Configuration Administrator** — This role enables the user to manage the configuration of systems in the organization using either the RHN website or the **Red Hat Network Configuration Manager**.
- **Monitoring Administrator** — This role allows for the scheduling of probes and oversight of other Monitoring infrastructure. This role is available only on Monitoring-enabled RHN Satellite Server version 3.6 or later.
- **Organization Administrator** — This role can perform any function available within Red Hat Network. As the master account for your organization, the person holding this role can alter the privileges of all other accounts, as well as conduct any of the tasks available to the other roles. Like the other roles, multiple Organization Administrators may exist.
- **System Group Administrator** — This role is one step below Organization Administrator in that it has complete authority over the systems and system groups to which it's granted access. This person can create new system groups, delete any assigned systems groups, add systems to groups, and manage user access to groups.

### 6.8.2. User List —

As shown in Figure 6-8, each row in the **User List** represents a user within your organization. There are three columns of information for each user:

- **Username** — The login name of the user. If you click on a username, the **User Details** page for the user is displayed. Refer to Section 6.8.2.2 *User Details* — for more information.
- **Real Name** — The full name of the user (last name first).
- **Roles** — List of the user's privileges, such as Organization Administrator, Channel Administrator and normal user. Users can have multiple roles.
- **Last Sign In** — Shows when the user last logged into RHN.

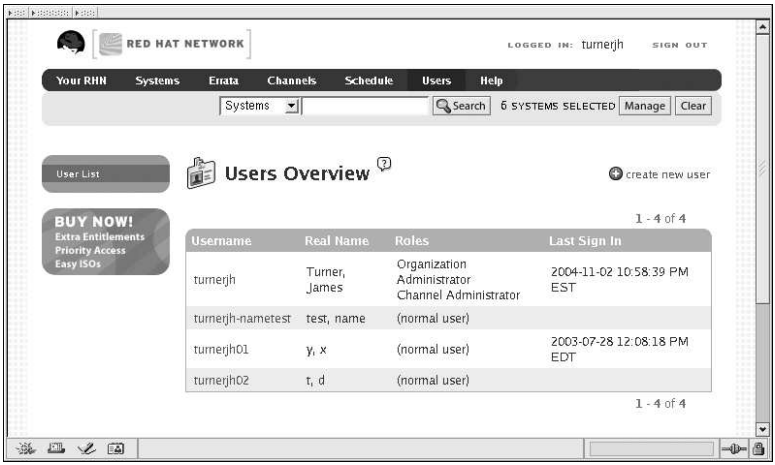


**Figure 6-8. User List**

### 6.8.2.1. Create User —

Click the **create new user** link on the top-right corner of the page to add new users to the organization. When registering a system, a user account can be created and added to the organization, as well. This should be coordinated by the Organization Administrator. Refer to Section 5.3 *Registering a User Account* for instructions.

On the **Create User** page, complete all required fields, including all login information. Then click the **Create Login** button on the bottom right-hand corner of the page. Once the login is created, you can click on the username in the **User List** to make system and group assignments. Refer to Section 6.8.2.2 *User Details* — for more information.

**Warning**

Be careful when creating users, because no interface exists for their deletion. Unless you are an RHN Satellite Server customer, you must contact Customer Service to have user accounts disabled. Go to the **Contact RHN** page at https://rhn.redhat.com/help/contact.pxt, select the Customer Service radio button, and enter your request containing the username to be removed and the overall account affected in the text fields before clicking **Send**. RHN Satellite Server customers may use the button on the **User Details** page.

### 6.8.2.2. User Details —

Clicking on a username displays the **User Details** page for the individual. This page is divided into the following tabs:

#### *6.8.2.2.1. User Details ⇒ Details* —

The username, first name, last name, email address, and user roles for the user. All of this information is modifiable. To do so, make your changes and click the **Update** button. Remember, when changing a user's password, you will see only asterisks as you type the password.

While it is possible for one Organization Administrator to remove Organization Administrator rights from another user, it is impossible to remove Organization Administrator rights from the sole remaining Organization Administrator. It is possible to remove your own Organization Administrator privileges so long as you are not the last Organization Administrator.

To assign a user a new role, select the appropriate checkbox. Remember that Organization Administrators are automatically granted administration access to all other roles, signified by grayed-out checkboxes. To grant a user the ability to manage the configuration of systems, select the **Configuration Administrator** checkbox. When satisfied with the changes, click **Update**.

#### *6.8.2.2.2. User Details ⇒ System Groups* —

List of system groups that the user may administer. To add or remove system groups from a user's administration, select or unselect the appropriate checkboxes and click the **Update Permissions** button.

In addition, you may establish default system groups for the user to capture all systems registered by that user. To do this, select the default group or groups from the dropdown menu at the bottom of the page. Then click the **Update Defaults** button. An asterisk appears next to the names of the defaults in the dropdown menu.

#### *6.8.2.2.3. User Details ⇒ Systems* —

List of systems that the user can administer. These systems come from the system groups assigned to the user on the previous tab. To add systems to the System Set Manager, select them and click the **Update** button. Clicking the name of a system takes you to its **System Details** page. Refer to Section 6.4.2.6 *System Details* for more information.

#### *6.8.2.2.4. User Details ⇒ Channel Permissions* —

Subscription and management options set in these subtabs (which correspond with similar tabs on the **Channel Details** and **Managed Channel Details** pages):

#### *6.8.2.2.4.1. User Details ⇒ Channel Permissions ⇒ Subscription* —

Identifies channels the user may subscribe systems to. To change these, select or unselect the appropriate checkboxes and click the **Update Permissions** button. Note that channels subscribable through the user's admin status or the channel's global setting cannot be altered. They are identified with a check icon.

#### *6.8.2.2.4.2. User Details ⇒ Channel Permissions ⇒ Management* —

Identifies channels the user may manage. To change these, select or unselect the appropriate checkboxes and click the **Update Permissions** button. This status does not enable the user to create new channels. Note that channels automatically manageable through the user's admin status cannot be altered. They are identified with a check icon. Remember, Organization Administrators and Channel Administrators can subscribe to or manage any channel.

#### 6.8.2.2.5. User Details ⇒ Preferences —

Modifiable Red Hat Network options. These include:

- Email Notification — Determine whether this user should receive email every time an Errata Alert is applicable to one or more systems in his or her RHN account, as well as daily summaries of system events.
- RHN List Page Size — Maximum number of items that will appear in a list on a single page. If more items are in the list, clicking the **Next** button will display the next group of items. This preference applies to the user's view of system lists, Errata lists, package lists, and so on.
- Time Zone — Set this user's time zone so that scheduled actions are arranged according to the time in the relevant time zone.
- Red Hat Contact Options — Identify what ways (email, phone, fax, or mail) Red Hat may contact the user.

To modify any of these options, make your changes and click the **Save Preferences** button.

#### 6.8.2.2.6. User Details ⇒ Addresses —

General address, billing address, and shipping address for the user, as configured during user creation. To modify these addresses, click **Edit this address** below the address to be modified, make the changes, and click the **Update** button.

#### 6.8.2.2.7. User Details ⇒ Notification Methods —

Email and pager addresses designated to receive alerts from Monitoring probes. To create a method, click **create new method** and complete the fields. If you will receive these alerts via pager, select the associated checkbox to have the messages sent in a shorter format. When finished, click **Create Method**. The method will show up in the Methods list, from which it can be edited and deleted.

You may delete notification methods here, as well. If the notification method has probes attached to it, you are presented with a list of the probes. Note that if you are a Monitoring Administrator and cannot manage the system in question, the **System Details** and probe's **Current State** page will not be accessible via links in their names. As always, Organization Administrator have full access to all aspects of your RHN account.

## 6.9. Monitoring —

If you click the **Monitoring** tab on the top navigation bar, the **Monitoring** category and links appear. These pages, which require Monitoring entitlements, enable you to view the results of probes you've set to run against Monitoring-entitled systems and manage the configuration of your monitoring infrastructure.

Initiate monitoring of a system through the **Probes** tab of the **System Details** page. Refer to Section 6.4.2.6 *System Details* for a description of the tab. See Appendix C *Probes* for the complete list of available probes.

### 6.9.1. Probe Status —

As shown in Figure 6-9, the **Probe Status** page is shown by default when you click **Monitoring** in the top navigation bar.

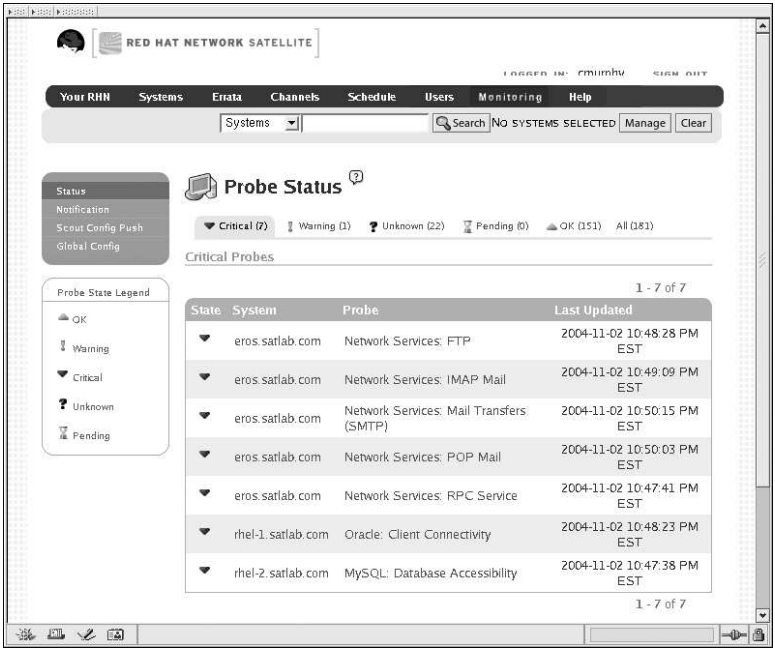


**Figure 6-9. Probe Status**

The **Probe Status** page displays the summary count of probes in the various states and provides a simple interface to find problematic probes quickly. Please note the probe totals in the tabs at the top of the page may not match the numbers of probes displayed in the tables below. The counts at the top include probes for all systems in your organization, while the tables display probes on only those systems to which you have access, through the System Group Administrator role. Also, the probe counts displayed here may be out of sync by as much as one minute.

The following list describes each state and identifies the icons associated with them:

- — *Critical* - The probe has crossed a CRITICAL threshold.
- — *Warning* - The probe has crossed a WARNING threshold.
- — *Unknown* - The probe is not able to accurately report metric or state data.
- — *Pending* - The probe has been scheduled but has not yet run or is unable to run.
- — *OK* - The probe is running successfully.

The **Probe Status** page contains tabs for each of the possible states, as well as one that lists all probes. The tables are identical in that each contains columns indicating probe state, the system being monitored, the probes used, and the date and time the status was last updated.

In these tables, clicking the name of the system takes you to the **Probes** tab of the **System Details** page. Clicking the name of the probe takes you to its **Current State** page. From there, you may edit the probe, delete it, and generate reports based upon its results.

#### 6.9.1.1. Probe Status ⇒ Critical —

The probes that have crossed their CRITICAL thresholds or reached a critical status by some other means. For instance, some probes go critical (rather than unknown) when exceeding their timeout period.

#### 6.9.1.2. Probe Status ⇒ Warning —

The probes that have crossed their WARNING thresholds.

#### 6.9.1.3. Probe Status ⇒ Unknown —

The probes that cannot collect the metrics needed to determine probe state. Most but not all probes enter an unknown state when exceeding their timeout period. This may mean that the timeout should be raised, or the connection cannot be established to the monitored system.

It is also possible the probes' configuration parameters are not correct and their data cannot be found. Finally, this state may indicate a software error has occurred.

#### 6.9.1.4. Probe Status ⇒ Pending —

The probes whose data have not been received by RHN. This state is expected for a probe that has just been scheduled but has not yet run. If all probes go into a pending state, your monitoring infrastructure may be failing.

#### 6.9.1.5. Probe Status ⇒ OK —

The probes that have run successfully without exception. This is the state desired for all probes.

#### 6.9.1.6. Probe Status ⇒ All —

All probes scheduled on systems in your account, listed in alphabetical order by the name of system.

#### 6.9.1.7. Current State —

Identifies the selected probe's status and when it last ran, while providing the ability to generate a report on the probe. Although this page is integral to monitoring, it is found under the **Probes** tab within the **System Details** page since its configuration is specific to the system being monitored.

To view a report of the probe's results, choose a relevant duration using the **date** fields and decide whether you would like to see metric data, the state change history or both. To obtain metric data, select the metric(s) you would like to be reported upon, and decide (using the checkboxes) whether

the results should be shown in a graph, an error log, or both. Then click **Generate report** at the bottom of the page. If no data exist for the probe's metrics, you are presented with a message indicating `No time series data found for specified time period`.

### 6.9.2. Notification —

Identifies the contact methods that have been established for your organization. These methods contain email or pager addresses designated to receive alerts from probes.

These methods are created within the **Notification Methods** tab of the **User Details** page. To see this tab, the user must first be granted the Monitoring Administrator or Organization Administrator role. Clicking the name of the contact method opens it for editing. Refer to Section 6.8.2.2 *User Details* — for instructions.

### 6.9.3. Scout Config Push —

Displays the status of your monitoring infrastructure. Anytime you make a change to your monitoring configuration, such as adding a probe to a system or editing a probe's thresholds, you must reconfigure your monitoring infrastructure. Do this by selecting the RHN Server's checkbox and clicking **Push Scout Configs**. The table on this page identifies the date and time of requested and completed pushes.

Clicking the name of the server opens its RHNMD SSH Public Key.

### 6.9.4. General Config —

Collects information that is universally applicable to your Monitoring infrastructure. The most important option available on this page in times of crisis is the **Silence All Notifications** checkbox. Selecting this will temporarily filter, or suspend, all notifications generated by your Monitoring infrastructure. Uncheck the box when you wish to resume notifications.

Modifying anything on this page will cause the Monitoring services on the RHN Satellite Server to reset, as well as schedule actions for the Monitoring services on all Monitoring-enabled RHN Proxy Servers that connect to this Satellite to be restarted. This is done so that the Monitoring services on these servers will reload their configuration immediately.

Typically, the defaults provided in other fields will do, since they were derived from your Satellite installation. Nevertheless, you may use the fields on this page to alter your Monitoring configuration. For instance, you may change your mail exchange server here. This page also allows you to alter the destination of all administrative emails from the Satellite. When finished, click **Update Config**.

# Chapter 7.
# Monitoring

The Red Hat Network Monitoring entitlement allows you to perform a whole host of actions designed to keep your systems running properly and efficiently. With it, you can keep close watch on system resources, network services, databases, and both standard and custom applications. (During the Monitoring technology preview, Provisioning-entitled systems are treated as if they have Monitoring entitlements.)

Monitoring provides both real-time and historical state-change information, as well as specific metric data. You are not only notified of failures immediately and warned of performance degradation before it becomes critical, but you are also given the information necessary to conduct capacity planning and event correlation. For instance, the results of a probe recording CPU usage across systems would prove invaluable in balancing loads on those systems.

Monitoring entails optionally establishing notification methods, installing probes on systems, regularly reviewing the status of all probes, and generating reports displaying historical data for a system or service. This chapter seeks to identify common tasks associated with the Monitoring entitlement. Remember, virtually all changes affecting your Monitoring infrastructure must be finalized by updating your configuration, through the **Scout Config Push** page.

## 7.1. Prerequisites

Before attempting to implement RHN Monitoring within your infrastructure, ensure you have all of the necessary tools in place. At a minimum, you need:

- Monitoring entitlements — These entitlements are required for all systems to be monitored (and are currently bundled with Provisioning entitlements). Monitoring is supported only on Red Hat Enterprise Linux systems. Entitlements may be obtained through the **Buy Now** links on the RHN website.
- RHN Satellite Server with Monitoring — Monitoring systems must be connected to a Satellite with a base operating system of Red Hat Enterprise Linux AS 3 Update 3 or later only. Refer to the RHN Satellite Server Installation Guide within **Help** for installation instructions. Contact a Red Hat sales representative to purchase Satellite.
- Monitoring Administrator — This role must be granted to users installing probes, creating notification methods, or altering the monitoring infrastructure in any way. (Remember, the Organization Administrator automatically inherits the abilities of all other roles within an organization and can therefore conduct these tasks.). Assign this role through the **User Details** page for the user.
- Red Hat Network Monitoring Daemon — This daemon is required on systems for probes monitoring internal processes to be executed. You may, however, be able to run these probes using the systems' existing SSH daemon (`sshd`). Refer to Section 7.2 *Red Hat Network Monitoring Daemon (`rhnmd`)* for installation instructions and a quick list of probes requiring this secure connection. Refer to Appendix C *Probes* for the complete list of available probes.

## 7.2. Red Hat Network Monitoring Daemon (`rhnmd`)

To get the most out of your Monitoring entitlement, Red Hat suggests installing the Red Hat Network Monitoring Daemon on your client systems. Based upon **OpenSSH**, `rhnmd` enables the RHN Satellite Server to communicate securely with the client system to access internal processes and retrieve probe status.

Please note the Red Hat Network Monitoring Daemon requires monitored systems allow connections on port 4545. You may avoid opening this port and installing the daemon altogether by using `sshd` instead. Refer to Section 7.2.3 *Configuring SSH* for details.

### 7.2.1. Probes requiring the daemon

An encrypted connection, either through the Red Hat Network Monitoring Daemon or `sshd`, is required on client systems for the following probes to run. Note that all probes in the Linux group have this requirement:

- Linux::CPU Usage
- Linux::Disk IO Throughput
- Linux::Disk Usage
- Linux::Inodes
- Linux::Interface Traffic
- Linux::Load
- Linux::Memory Usage
- Linux::Process Counts by State
- Linux::Process Count Total
- Linux::Process Health
- Linux::Process Running
- Linux::Swap Usage
- Linux::TCP Connections by State
- Linux::Users
- Linux::Virtual Memory
- LogAgent::Log Pattern Match
- LogAgent::Log Size
- Network Services::Remote Ping
- Oracle::Client Connectivity
- General::Remote Program
- General::Remote Program with Data

### 7.2.2. Installing the Red Hat Network Monitoring Daemon

Install the Red Hat Network Monitoring Daemon to prepare systems for monitoring using the probes identified in Section 7.2.1 *Probes requiring the daemon*. Note that the steps in this section are optional if you intend to use `sshd` to allow secure connections between the RHN monitoring infrastructure and the monitored systems. Refer to Section 7.2.3 *Configuring SSH* for instructions.

The `rhnmd` package can be found in the RHN Tools channel for all Red Hat Enterprise Linux distributions. To install it:

1. Subscribe the systems to be monitored to the RHN Tools channel associated with the system, if they already aren't. This can be done individually through the **System Details** ⇒ **Channels** ⇒ **Software** subtab or to multiple systems at once through the **Channel Details** ⇒ **Target Systems** tab.

2. Once subscribed, open the **Channel Details** ⇒ **Packages** tab and find the `rhnmd` package (under 'R').
3. Click the package name to open the **Package Details** page. Go to the **Target Systems** tab, select the desired systems, and click **Install Packages**.
4. Install the SSH public key on all client systems to be monitored, as described in Section 7.2.4 *Installing the SSH key*.
5. Start the Red Hat Network Monitoring Daemon on all client systems using the command:
   `service rhnmd start`
6. When adding probes requiring the daemon, accept the default values for **RHNMD User** and **RHNMD Port**: **`nocpulse`** and **`4545`**, respectively.

### 7.2.3. Configuring SSH

If you wish to avoid installing the Red Hat Network Monitoring Daemon and opening port 4545 on client systems, you may configure `sshd` to provide the encrypted connection required between the systems and RHN. This may be especially desirable if you already have `sshd` running. To configure the daemon for monitoring use:

1. Ensure the SSH package is installed on the systems to be monitored:
   `rpm -qi ssh`
2. Identify the user to be associated with the daemon. This can be any user available on the system, as long as the required SSH key can be put in the user's `~/.ssh/authorized_keys` file.
3. Identify the port used by the daemon, as identified in its `/etc/ssh/sshd_config` configuration file. The default is port 22.
4. Install the SSH public key on all client systems to be monitored, as described in Section 7.2.4 *Installing the SSH key*.
5. Start the `sshd` on all client systems using the command:
   `service sshd start`
6. When adding probes requiring the daemon, insert the values derived from steps 2 and 3 in the **RHNMD User** and **RHNMD Port** fields.

### 7.2.4. Installing the SSH key

Whether you use `rhnmd` or `sshd`, you must install the Red Hat Network Monitoring Daemon public SSH key on the systems to be monitored to complete the secure connection. To install it:

1. In the RHN website, navigate to the **Monitoring** ⇒ **Scout Config Push** page and click the name of the RHN Server that will monitor the client system. The SSH `id_dsa.pub` key is visible on the resulting page.
2. Copy the character string (beginning with `ssh-dss` and ending with the hostname of the RHN Server).
3. On the command line of the system to be monitored, switch to the user aligned with the daemon. This is accomplished for `rhnmd` with the command:
   `su - nocpulse`
4. Paste the key character string into the `~/.ssh/authorized_keys` file for the daemon's user. For `rhnmd`, this is `/opt/nocpulse/.ssh/authorized_keys`.

If config management is enabled on the systems to be monitored, you may deploy this file across systems using a config channel. Refer to Section 6.6.6.1 *Preparing Systems for Config Management* for details.

**Note**

If valid entries already exist in `authorized_keys`, add the daemon key to the file rather than use it to replace it. Do this by saving the copied text to `id_dsa.pub` in the same `.ssh/` directory and then running the command: `cat ~/.ssh/id_dsa.pub >> ~/.ssh/authorized_keys`.

5. Finally, ensure the `.ssh/` directory and `authorized_keys` file have the appropriate permissions set. This can be done as the daemon's user with the following commands:

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```

Once the key is in place and accessible, all probes that require it should begin to allow `ssh` connections between the Monitoring infrastructure and the monitored system. You may then schedule probes requiring the monitoring daemon to run against the newly configured systems.

## 7.3. Notifications

In addition to viewing probe status within the RHN interface, you may be notified whenever a probe changes state. This is especially important when monitoring mission-critical production systems. For this reason, Red Hat recommends taking advantage of this feature.

To enable probe notifications within RHN, you must have identified a mail exchange server and mail domain during installation of your RHN Satellite Server and configured **sendmail** to properly handle incoming mail. Refer to the Installation chapter of the *RHN Satellite Server Installation Guide* for details.

### 7.3.1. Creating Notification Methods

Notifications are sent to a *notification method*, in essence an email or pager address associated with a specific RHN user. Although the address is tied to a particular user account, it may serve multiple administrators through an alias or mailing list. And each user account can contain multiple notification methods. To create a notification method:

1. Log into the RHN website as either an Organization Administrator or Monitoring Administrator.
2. Navigate to the **User Details** ⇒ **Notification Methods** tab and click **create new method**.
3. Enter an intuitive, descriptive label for the method name, such as **`DBA day email`**, provide the correct email or pager address. Remember, the labels for all notification methods will be available in a single list during probe creation, so they should be unique to your organization.
4. Select the checkbox if you desire abbreviated messages to be sent to the pager. This shorter format contains only the probe state, system hostname, probe name, time of message, and Send ID. The standard, longer format displays additional message headers, system and probe details, and instructions for response.
5. When finished, click **Create Method**. The new method shows up in the **User Details** ⇒ **Notification Methods** tab and the **Notification** page under the top **Monitoring** category. Click its name to edit or delete it.

6. While adding probes, select the **Probe Notifications** checkbox and select the new notification method from the resulting pulldown menu. Understand that notification methods assigned to probes cannot be deleted until that association has been removed.

### 7.3.2. Receiving Notifications

If you create notification methods and associate them with probes, you must be prepared to receive them. These notifications will come in the form of brief text messages sent to either email or pager addresses. Here is an example of an email notification:

```
Subject: CRITICAL: [hostname]: Satellite: Users at 1
From: "Monitoring Satellite Notification" (rogerthat01@redhat.com)
Date: Mon, 6 Dec 2004 13:42:28 -0800
To: user@organization.com

This is RHN Monitoring Satellite notification 01dc8hqw.

Time: Mon Dec 06, 21:42:25 PST
State: CRITICAL
System: [hostname] ([IP address])
Probe: Satellite: Users
Message: Users 6 (above critical threshold of 2)
Notification #116 for Users

Run from: RHN Monitoring Satellite
```

As you can see, the longer email notifications contain virtually everything you would need to know about the associated probe. In addition to the probe command, run time, system monitored, and state, the message contains the *Send ID*, which is a unique character string representing the precise message and probe. In the above message, the Send ID is `01dc8hqw`.

Pager notifications, by necessity, contain only the most important details, namely the subject of the email message (containing state, system, probe, and time) and the Send ID. Here is an example pager notification:

```
CRITICAL: [hostname]: Satellite: Users at 21:42 PST, notification 01dc8hqw
```

### 7.3.3. Redirecting Notifications

Upon receiving a notification, you may redirect it by including advanced notification rules within an acknowledgement email. Just reply to the notification and include the desired option. These are the possible redirect options, or *filter types*:

- ACK METOO — Sends the notification to the redirect destination(s) *in addition to* the default destination.
- ACK SUSPEND — Sends the notification to nobody *instead of* the default destination.
- ACK AUTOACK — Does not change the destination of the notification, but automatically acknowledges matching alerts as soon as they are sent to prevent escalations.
- ACK REDIR — Sends the notification to the redirect destination(s) *instead of* the default destination.

The format of the rule should be *`filter_type probe_type duration email_address`* where filter type equals one of the following advanced commands, probe type equals probe or system, duration equals the length of time for the redirect, and email address equals the intended recipient. For example:

```
ACK METOO system 1h boss@domain.com
```

Capitalization is not required. Duration can be listed in minutes (m), hours (h), or days (d). Email addresses are needed only for redirects (REDIR) and supplemental (METOO) notifications.

The description of the action contained in the resulting email will default to the precise command entered by the user. The reason listed will be a summary of the action, such as `email ack redirect by user@domain.com` where user equals the sender of the email.

### 7.3.4. Filtering Notifications

Since notifications can be generated whenever a probe changes state, simple changes in your network can result in a flood of notifications. Although Red Hat recommends installing your own mail filters to appropriately route and flag these messages, we also recognize the need to outright halt them.

To this end, Red Hat Network offers the **Silence All Notifications** mechanism. This checkbox can be found within the **Monitoring** category of the RHN website, within the **General Config** page.

To temporarily filter, or suspend, all notifications generated by your Monitoring infrastructure, select the **Silence All Notifications** checkbox, and click **Update Config**. To restore notifications, uncheck the box and once again update your configuration.

### 7.3.5. Deleting Notification Methods

Theoretically, removing notification methods should be as easy if not easier than creating them. After all, you must populate no fields to conduct the deletion and a button exists for this explicit purpose. But existing relationships between methods and probes can complicate this process. These steps walk you through it:

1. Log into the RHN website as an Organization Administrator.
2. Navigate to the **Monitoring** ⇒ **Notifications** page and click the name of the method to be removed.
3. On the **User Details** ⇒ **Notification Methods** tab, click **delete method**. If the method isn't associated with any probes, you are presented with a confirmation page. Click **Confirm Deletion**. The notification method is removed.

**Tip**

Since both the notification method name and address can be edited, consider updating the method rather than deleting it. This will redirect notifications from all probes using the method without having to edit each probe and create a new notification method.

4. If the method is associated with one or more probes, instead of a confirmation page, you are presented with a list of the probes using the method and the systems to which the probes are attached. Click the probe name to go directly to the **System Details** ⇒ **Probes** tab.
5. On the **System Details** ⇒ **Probes** tab, select another notification method and click **Update Probe**.
6. You may now return to the **Monitoring** ⇒ **Notifications** page and delete the notification method.

## 7.4. Probes

Now that the Red Hat Network Monitoring Daemon has been installed and notification methods have been created, you may begin installing probes on your Monitoring-entitled systems. If a system is entitled to Monitoring, a **Probes** tab appears within its **System Details** page. It is here where you will conduct most probe-related work.

### 7.4.1. Managing Probes

To add a probe to the system, it must be entitled to Monitoring (although Provisioning-entitled systems may be monitored during the entitlement's technology preview). Further, you must have access to the system itself, either as the system's individual administrator, through the System Group Administrator role, or as the Organization Administrator. Then:

1. Log into the RHN website as either an Organization Administrator or the System Group Administrator for the system.
2. Navigate to the **System Details** ⇒ **Probes** tab and click **create new probe**.
3. On the **System Probe Creation** page, complete all required fields. First, select the Probe Command Group. This alters the list of available probes and other fields and requirements. Refer to Appendix C *Probes* for the complete list of probes by command group. Remember that some probes require the Red Hat Network Monitoring Daemon to be installed on the client system.
4. Select the desired Probe Command and the Monitoring Scout, typically **`RHN Monitoring Satellite`** but possibly an RHN Proxy Server. Enter a brief but unique description for the probe.
5. Select the Probe Notifications checkbox to receive notifications when the probe changes state. Use the Probe Check Interval pulldown menu to determine how often notifications should be sent. Selecting **`1 minute`** (and the **Probe Notification** checkbox) means you will receive notifications every minute the probe surpasses its CRITICAL or WARNING thresholds. Refer to Section 7.3 *Notifications* to find out how to create notification methods and acknowledge their messages.
6. Use the RHNMD User and RHNMD Port fields, if they appear, to force the probe to communicate via `sshd`, rather than the Red Hat Network Monitoring Daemon. Refer to Section 7.2.3 *Configuring SSH* for details. Otherwise, accept the default values of **`nocpulse`** and **`4545`**, respectively.
7. If the Timeout field appears, review the default value and adjust to meet your needs. Most but not all timeouts result in an UNKNOWN state. If the probe's metrics are time-based, ensure the timeout is not less than the time alloted to thresholds. Otherwise, the metrics serve no purpose, as the probe will time out before any thresholds are crossed.
8. Use the remaining fields to establish the probe's alert thresholds, if applicable. These CRITICAL and WARNING values determine at what point the probe has changed state. Refer to Section 7.4.2 *Establishing Thresholds* for best practices regarding these thresholds.
9. When finished, click **Create Probe**. Remember, you must commit your Monitoring configuration change on the **Scout Config Push** page for this to take effect.

To delete a probe, navigate to its **Current State** page (by clicking the name of the probe from the **System Details** ⇒ **Probes** tab), and click **delete probe**. Then confirm the deletion.

### 7.4.2. Establishing Thresholds

Many of the probes offered by RHN contain alert thresholds that, when crossed, indicate a change in state for the probe. For instance, the Linux::CPU Usage probe allows you to set CRITICAL and WARNING thresholds for the percent of CPU used. If the system being monitored reports 75 percent

of its CPU used, and the WARNING threshold is set to 70 percent, the probe will go into a WARNING state. Some probes offer a multitude of such thresholds.

In order to get the most out of your Monitoring entitlement and avoid false notifications, Red Hat recommends running your probes without notifications for a time to establish baseline performance for each of your systems. Although the default values provided for probes may suit you, every organization has a different environment that may require altering thresholds.

### 7.4.3. Monitoring the RHN Server

In addition to monitoring all of your client systems, you may also use RHN to monitor your RHN Server itself, whether that be an RHN Satellite Server an RHN Proxy Server or both. To monitor your RHN Server, find a system monitored by the server, and go to that system's **System Details** ⇒ **Probes** tab.

Click **create new probe** and select the **Satellite** Probe Command Group. Then complete the remaining fields as you would for any other probe. Refer to Section 7.4.1 *Managing Probes* for instructions.

Although the RHN Server will appear to be monitored by the client system, the probe will actually be run from the server on itself. Thresholds and notifications will work normally.

## 7.5. Troubleshooting

Though all Monitoring-related activities are conducted through the RHN website, Red Hat provides access to some command line diagnostic tools that may help you determine the cause of errors. To use these tools, you must be able to become the **nocpulse** user on the RHN Server conducting the monitoring.

First log into the RHN Server as root. Then switch to the **nocpulse** user with the following command:

```
su - nocpulse
```

You may now use the diagnostic tools described within the rest of this section.

### 7.5.1. Examining Probes with `rhn-catalog`

To thoroughly troubleshoot a probe, you must first obtain its probe ID. You may get this by running `rhn-catalog` on the RHN Server as the **nocpulse** user. The output will resemble:

```
2 ServiceProbe on example1.redhat.com (199.168.36.245): test 2
3 ServiceProbe on example2.redhat.com (199.168.36.173): rhel2.1 test
4 ServiceProbe on example3.redhat.com (199.168.36.174): SSH
5 ServiceProbe on example4.redhat.com (199.168.36.175): HTTP
```

The probe ID is the first number in the line, while the probe name (as entered in the RHN website) is the final entry on the line. For example, the `5` probe ID corresponds to the probe named `HTTP`.

Further, you may pass the `--commandline` (`-c`) and `--dump` (`-d`) options along with a probe ID to `rhn-catalog` to obtain additional details about the probe, like so:

```
rhn-catalog --commandline --dump 5
```

The `--commandline` option yields the command parameters set for the probe, while `--dump` retrieves everything else, including alert thresholds and notification intervals and methods.

The command above will result in output similar to:

```
5 ServiceProbe on example4.redhat.com (199.168.36.175  ):
linux:cpu usage
      Run as: Unix::CPU.pm --critical=90 --sshhost=199.168.36.175
--warn=70 --timeout=15 --sshuser=nocpulse
--shell=SSHRemoteCommandShell --sshport=4545
```

Now that you have the ID, you use it with `rhn-rhnprobe` to examine the probe's output. Refer to Section 7.5.2 *Viewing the output of `rhn-runprobe`* for instructions.

### 7.5.2. Viewing the output of `rhn-runprobe`

Now that you've obtained the probe ID with `rhn-catalog`, you can use it in conjunction with `rhn-runprobe` to examine the complete output of the probe. Note that by default, `rhn-runprobe` works in test mode, meaning no results are entered in the database. Here are its options:

| Option | Description |
|---|---|
| `--help` | List the available options and exit. |
| `--probe=`*`PROBE_ID`* | Run the probe with this ID. |
| `--prob_arg=`*`PARAMETER`* | Override any probe parameters from the database. |
| `--module=`*`PERL_MODULE`* | Package name of alternate code to run. |
| `--log=all=`*`LEVEL`* | Sets log level for a package or package prefix. |
| `--debug=`*`LEVEL`* | Sets numeric debugging level. |
| `--live` | Executes the probe and both enqueues data and sends out notifications (if needed). |

**Table 7-1. `rhn-runprobe` Options**

At a minimum, you should include the `--probe` and `--log` options and values. The probe ID satisfies the former, while the latter should be populated with **`all`** to request output from all run levels and the numeric level of verbosity. Here is an example:

```
rhn-runprobe --probe=5 --log=all=4
```

More specifically, you may provide the command parameters derived from `rhn-catalog`, like so:

```
rhn-runprobe 5 --log all=4 --sshuser=nocpulse --sshport=4545
```

This will yield verbose output depicting the probe's attempted run. Errors are clearly identified.

# Appendix A. Command Line Config Management Tools

In addition to the options provided in the RHN website, Red Hat Network offers two command line tools for managing configuration files: the **Red Hat Network Configuration Client** and the **Red Hat Network Configuration Manager**. If you don't yet have these these tools installed, they can be found within the RHN Provisioning child channel for your operating system.

**Tip**

Keep in mind, whenever a configuration file is deployed via RHN, a backup of the previous file including its full path is made in the `/var/lib/rhncfg/backups/` directory on the affected system. The backup will retain its filename but have a `.rhn-cfg-backup` extension appended.

## A.1. Red Hat Network Configuration Client

As the name implies, the **Red Hat Network Configuration Client** (`rhncfg-client`) is to be installed and run from an individual client system. From there you may use it to gain knowledge about how RHN will deploy configuration files to the particular system.

The **Red Hat Network Configuration Client** offers these primary modes: list, get, channels, diff, and verify.

### A.1.1. Listing Config Files

To list the configuration files for the machine and the labels of the config channels containing them, issue the command:

```
rhncfg-client list
```

You should see output resembling:

```
     Config Channel   File
  config-channel-17   /etc/foo.txt
  config-channel-17   /var/spool/aalib.rpm
  config-channel-14   /etc/foo.txt
```

### A.1.2. Getting a Config File

To download the most relevant configuration file for the machine, issue the command:

```
rhncfg-client get /etc/foo.txt
```

You should see output resembling:

```
Deploying /etc/foo.txt
```

You may then `more` the file to view its contents. Note that the file is selected as most relevant based upon the rank of the config channel containing it. This is accomplished within the **Configuration** tab of the **System Details** page. Refer to Section 6.4.2.6 *System Details* for instructions.

### A.1.3. Viewing Config Channels

To view the labels and names of the config channels that apply to the system, issue the command:

```
rhncfg-client channels
```

You should see output resembling:

```
Config channels:
Label                          Name
-----                          ----
config-channel-17              config chan 2
config-channel-14              config chan 1
```

### A.1.4. Differentiating between Config Files

To obtain a difference between the config files deployed on the system and those for it stored by RHN, issue the command:

```
rhncfg-client diff
```

You should see output resembling:

```
--- /tmp/@3603.0.rhn-cfg-tmp    2004-01-13 14:18:31.000000000 -0500
+++ /etc/foo.txt        2003-12-16 21:35:32.000000000 -0500
@@ -1,3 +1,5 @@
+blaaaaaaaaaaaaaaah
```

In addition, you may include the `--topdir` option to compare config files in RHN with those located in an arbitrary (and unused) location on the system, like so:

```
[root@ root]# rhncfg-client diff --topdir /home/test/blah/
/usr/bin/diff: /home/test/blah/etc/foo.txt: No such file or
directory
/usr/bin/diff: /home/test/blah/var/spool/aalib.rpm: No such file or
directory
```

### A.1.5. Verifying Config Files

To quickly determine if files are different than those associated with it in RHN, issue the command:

```
rhncfg-client verify
```

You should see output resembling:

```
 modified /etc/foo.txt
          /var/spool/aalib.rpm
```

The file `foo.txt` is locally modified, while `aalib.rpm` is not.

## A.2. Red Hat Network Configuration Manager

Unlike the **Red Hat Network Configuration Client**, the **Red Hat Network Configuration Manager** (`rhncfg-manager`) is designed to maintain RHN's central repository of config files and channels, not those located on client systems. This tool offers a command line alternative to the configuration management features within the RHN website, as well as the ability to script some or all of the related maintenance.

It is intended for use by Config Administrators and in fact requires an RHN username and password that has the appropriate permission set. The username may be specified in `/etc/sysconfig/rhn/rhncfg-manager.conf` or in the [rhncfg-manager] section of `~/.rhncfgrc`.

When the **Red Hat Network Configuration Manager** is run as root, it attempts to pull in needed configuration values from the **Red Hat Update Agent**. When run as something other than root, you may have to make configuration changes within the `~/.rhncfgrc` file. The session file is cached in `~/.rhncfg-manager-session` to prevent logging in for every command.

The default timeout for the **Red Hat Network Configuration Manager** is 30 minutes. To alter this, add the `server.session_lifetime` option and new value to the `/etc/rhn/rhn.conf` file on the server running the manager, like so:

```
server.session_lifetime = 120
```

The **Red Hat Network Configuration Manager** offers these primary modes: add, create-channel, diff, diff-revisions, download-channel, get, list, list-channels, remove, remove-channel, revisions, update, and upload-channel.

Each mode offers its own set of options, which can be seen by issuing the command, `rhncfg-manager` *`mode`* `--help`, such as:

```
rhncfg-manager diff-revisions --help
```

You can see such a list of options for the add mode at Section A.2.2.1 *Add Options*.

### A.2.1. Creating a Config Channel

To create a config channel for your organization, issue the command:

```
rhncfg-manager create-channel channel-label
```

If prompted for your RHN username and password, provide them. You should see output resembling:

```
Red Hat Network username: rhn-user
Password:
Creating config channel channel-label
Config channel channel-label created
```

Once you've created a config channel, you have the remaining modes available for populating and maintaining that channel.

### A.2.2. Adding Files to a Config Channel

To add a file to a config channel, you need to specify the channel label, as well as the local file to be uploaded, such as:

```
rhncfg-manager add
   --channel=channel-label
   /path/to/file
```

In addition to the required channel label and path to the file, you may use the available options for modifying the file during its addition. For instance, you may alter the path and filename by including the `--dest-file` option in the command, like:

```
rhncfg-manager add
   --channel=channel-label
   --dest-file=/new/path/to/file.txt
   /path/to/file
```

You should see output resembling:

```
Pushing to channel blah
Local file >/path/to/file -> remote file /new/path/to/file.txt
```

#### A.2.2.1. Add Options

The following options are applicable to the add mode:

| Option | Description |
|---|---|
| `-h, --help` | Display this list of options and exits. |
| `-c=, --channel=CHANNEL_LABEL` | *Required* - Use this config channel. |
| `-d=, --dest-file=DEST_FILE` | *Conflicts with --topdir* - Identify the destination path and filename of a single file. |
| `-t=, --topdir=TOPDIR` | *Conflicts with --dest-file* - Handle multiple files at a different location than their destination path. Make all files relative to this string. |
| `--delim-start=DELIM_START` | Start delimiter for variable interpolation. |
| `--delim-end=DELIM_END` | End delimiter for variable interpolation. |

**Table A-1. Add Options**

### A.2.3. Differentiating between Latest Config Files

To obtain a difference between the config files on disk and the latest revisions in a channel, issue the command:

```
rhncfg-manager diff
   --channel=channel-label
   --dest-file=/path/to/file.txt
   /local/path/to/file
```

You should see output resembling:

```
/tmp/dest_path/foo.txt /home/test/blahhello_world.txt
--- /tmp/dest_path/foo.txt      config_channel: blah   revision: 1
+++ /home/test/blah/hello_world.txt   2003-12-14 19:08:59.000000000
-0500
@@ -1 +1 @@
-foo
+hello, world
```

### A.2.4. Differentiating between Various Versions

To compare different versions of a file across channels and revisions, use the `-r` flag to indicate which revision of the file should be compared and the `-n` flag to identify the two channels to be checked. Refer to Section A.2.11 *Determining the Number of File Revisions* for related instructions. Note that you specify only one filename here, since you're comparing the file against another version of itself, such as:

```
rhncfg-manager diff-revisions
   -n=channel-label1
   -r=1
   -n=channel-label2
   -r=1
   /path/to/file.txt
```

You should see output resembling:

```
--- /tmp/dest_path/foo.txt      2004-01-13 14:36:41     config
channel: blah2  revision: 1
--- /tmp/dest_path/foo.txt      2004-01-13 14:42:42     config
channel: blah3  revision: 1
@@ -1 +1,20 @@
-foo
+blaaaaaaaaaaaaaaah
+-----BEGIN PGP SIGNATURE-----
+Version: GnuPG v1.0.6 (GNU/Linux)
+Comment: For info see http://www.gnupg.org
+
+iD8DBQA9ZY6vse4XmfJPGwgRAsHcAJ9ud9dabUcdscdcqB8AZP7e0Fua0NmKsdhQCeOWHX
+VsDTfen2NWdwwPaTM+S+Cow=
+=Ltp2
+-----END PGP SIGNATURE-----
```

### A.2.5. Downloading All Files in a Channel

To download all the files in a channel to disk, create a directory and issue the command:

```
rhncfg-manager download-channel channel-label --topdir .
```

You should see output resembling:

```
Copying /tmp/dest_path/foo.txt -> blah2/tmp/dest_path/foo.txt
```

### A.2.6. Getting the Contents of a File

To get the contents of a particular file to stdout, issue the command:

```
rhncfg-manager get
   --channel=channel-label
   /tmp/dest_path/foo.txt
```

You should see the contents of the file as output.

### A.2.7. Listing All Files in a Channel

To list all the files in a channel, issue the command:

```
rhncfg-manager list channel-label
```

You should see output resembling:

```
Files in config channel 'blah3':
  /tmp/dest_path/foo.txt
```

### A.2.8. Listing All Config Channels

To list all of your organization's configuration channels, issue the command:

```
rhncfg-manager list-channels
```

You should see output resembling:

```
Available config channels:
  blah
  blah2
  blah3
  config-channel-14
  config-channel-17
```

Note that this does not list local_override or server_import channels.

### A.2.9. Removing a File from a Channel

To remove a file from a channel, issue the command:

```
rhncfg-manager remove
   --channel=channel-label
   /tmp/dest_path/foo.txt
```

If prompted for your RHN username and password, provide them. You should see output resembling:

```
Red Hat Network username: rhn-user
Password:
Removing from config channel blah3
/tmp/dest_path/foo.txt removed
```

### A.2.10. Deleting a Config Channel

To detroy a config channel in your organization, issue the command:

```
rhncfg-manager remove-channel channel-label
```

You should see output resembling:

```
Removing config channel blah
Config channel blah removed
```

### A.2.11. Determining the Number of File Revisions

To find out how many revisions (revisions go from 1 to N with N being an integer greater than 0) of a file/path are in a channel, issue the command:

```
rhncfg-manager revisions channel-label /tmp/dest_path/foo.txt
```

You should see output resembling:

```
Analyzing files in config channel blah
/tmp/dest_path/foo.txt: 1
```

### A.2.12. Updating a File in a Channel

To create a new revision of a file in a channel (or add the first revision to that channel if none existed before for the given path), issue the command:

```
rhncfg-manager update
   --channel=channel-label
   --dest-file=/path/to/file.txt
   /local/path/to/file
```

You should see output resembling:

```
Pushing to channel blah:
Local file blah/tmp/dest_path/foo.txt -> remote file /tmp/dest_path/foo.txt
```

### A.2.13. Uploading Multiple Files at Once

To upload multiple files to a config channel from local disk at once, issue the command:

```
rhncfg-manager upload-channel
   --topdir=topdir
   channel-label
```

You should see output resembling:

```
Using config channel blah4
Uploading /tmp/ola_world.txt from blah4/tmp/ola_world.txt
```

# Appendix B.

# RHN API Access

In an effort to provide customers with added flexibility, RHN makes an application programming interface (API) available. This interface can be found by clicking **Help** at the top-right corner of the RHN website, then clicking **API** in the left navigation bar. Or you may go directly to: https://rhn.redhat.com/rpc/api/. You should use this URL for your XMLRPC server, as well as your browser.

**Warning**

This API should be considered experimental and used strictly for evaluation by advanced users. Red Hat strongly discourages you from using this interface to alter production systems, unless you are sure your changes will not result in errors.

The RHN API is based upon XML-RPC, which allows distinct pieces of software on disparate systems to make remote procedure calls using XML over HTTP. For this reason, any calls you make are expected to meet the constraints of XML-RPC. You can find out more at http://www.xmlrpc.com/.

Because the RHN API is self-documenting and subject to change, this section bypasses a list of classes and methods (which can be found within the interface) in favor of tips for using the API efficiently. These include steps for determining required values and a sample script that makes some of the calls.

## B.1. Using the auth Class and Getting the Session

It is worth noting you will almost invariably use the auth class first. This class offers a single method, login. Use this to establish an RHN session. It requires values for three parameters: username, password, and duration. The first two come directly from your RHN account, while the third is the length of time the session should last in seconds, typically 1200. It will return a session string than can be used in all other methods.

## B.2. Obtaining the system_id

Many of the methods require a value for the system_id parameter. This is the unique alphanumeric value assigned to each system when registered to RHN. It can be found within the `/etc/sysconfig/rhn/systemid` file on the machine. In addition, you may use the download_system_id method within the system class to obtain the value.

## B.3. Determining the sid

Several methods require a value for the sid, or server ID, parameter. Note that this is different from the system_id. You may determine the sid of a machine in two different ways. First, you can log into the RHN website, click the name of a system, and view the sid at the end of the URL in the location bar. It will be after the equal (=) sign in something like, "index.pxt?sid=1003486534". Second, you may use the list_user_systems method within the system class to obtain a list of systems available to the user that contains the associated sids.

## B.4. Viewing the cid

Like servers, channels have their own IDs. This value, the cid, is a required parameter for some methods, including set_base_channel and set_child_channels. Also like the sid, the cid can be obtained through the RHN website. Just click on the name of a channel and view the end of the URL, something like, "details.pxt?cid=54".

## B.5. Getting the sgid

System groups join servers and channels in having their own IDs. This value, the sgid, is a required parameter for the set_group_membership method, for instance. Like the sid and cid, the sgid can be obtained through the RHN website. Just click on the name of a system group and view the end of the URL, something like, "details.pxt?sgid=334958". Note that the member parameter within the set_group_membership method requires only yes or no as input to make the association.

## B.6. Sample API Script

The following sample script depicts how an RHN API client should be constructed. Review the comments and links for a full discussion of the calls made.

```
#!/usr/bin/perl -w

use strict;
use Frontier::Client;
use Data::Dumper;

##########################################################################
# This is a sample script for use of the experimental RHN Management APIs. #
# The API is currently available using XMLRPC only, which is described in  #
# depth at:                                                                #
#                                                                          #
# http://www.xmlrpc.com/                                                   #
#                                                                          #
# We use the Frontier modules, available from:                             #
#                                                                          #
# http://theoryx5.uwinnipeg.ca/mod_perl/cpan-search?dist=Frontier-RPC      #
#                                                                          #
##########################################################################


##########################################################################
#   Defining an XMLRPC session.                                            #
##########################################################################

# Define the host first.  This will be the FQDN of your satellite system.
my $HOST = 'satellite.server.yourdomain.com';

# Now we create the client object that will be used throughout the session.

my $client = new Frontier::Client(url => "http://$HOST/rpc/api");

# Next, we execute a login call, which returns a session identifier that will
# be passed in all subsequent calls.  The syntax of this call is described at:
#
#   http://$HOST/rpc/api/auth/login/

my $session = $client->call('auth.login', 'username', 'password');
```

```
##############################################################################
#   System calls.                                                            #
##############################################################################

# This next call returns a list of systems available to the user.  The
# syntax of this call is described at:
#
#   http://$HOST/rpc/api/system/list_user_systems/
#
# In the code snippet below, we dump data about our systems, and we
# capture the ID of the first system we find for future operations.

my $systems = $client->call('system.list_user_systems', $session);
for my $system (@$systems) {
  print Dumper($system);
}
print "\n\nCapturing ID of system @$systems[0]->{name}\n\n";
my $systemid = @$systems[0]->{id};

# This next call returns a list of packages present on this system.  The
# syntax of this call is described at:
#
#   http://$HOST/rpc/api/system/list_packages/
#
# This will probably be a pretty long list.

my $packages = $client->call('system.list_packages', $session, $systemid);
for my $package (@$packages) {
  print Dumper($package);
}

# Additional system calls are described at:
#   http://$HOST/rpc/api/system/
```

# Appendix C.

# Probes

As described in Section 6.9 *Monitoring* — , systems entitled with Monitoring can have probes applied against them to constantly confirm their health and full operability. This appendix lists the available probes broken down by command group, such as Apache.

Many probes that monitor internal aspects of your systems, rather than externally facing components such as `httpd`, require the installation of the Red Hat Network Monitoring Daemon (`rhnmd`). This requirement is noted within the individual probe reference.

Each probe has its own reference that identifies required fields (marked with *), default values, and the thresholds that may be set to trigger alerts. Similarly, the beginning of each command group's section contains information applicable to all probes in that group. But before we begin examining individual probes, let's cover general guidelines for them all.

**Note**

Nearly all of the probes use *Transmission Control Protocol* (TCP) as their transport protocol. Exceptions to this are noted within the individual probe references.

## C.1. Probe guidelines

The purpose of each probe is to obtain metrics from and identify the status of the system or application being monitored. To accomplish this, first review the probe descriptions in this appendix. Then apply relevant probes to Monitoring-entitled systems within your organization, as described in Section 6.9 *Monitoring* — .

While adding those probes, select meaningful thresholds that when crossed notify you and your administrators of problems within your infrastructure. All probes that have been scheduled but are not yet running show a PENDING status in the **Status Bar**, while those with successful results not exceeding any thresholds display an OK status. Note that thresholds can be minimums, maximums, or both, depending on the probe.

A CRITICAL status is reported for the probe if it returns a value exceeding its critical threshold, while a WARNING status is returned for metrics beyond the warning threshold. Probes not run on the target system within the selected timeout period usually result in an UNKNOWN status, but not always. Timeout periods are entered in seconds, unless otherwise indicated. Exceptions to these rules are noted within the individual probe references.

**Important**

Some probes have thresholds based upon time. In order for CRITICAL and WARNING thresholds based upon time to work as intended, their values cannot exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status will be returned in all instances of extended latency, thereby nullifying the thresholds. For this reason, Red Hat strongly recommends ensuring timeout periods exceed all timed thresholds.

## C.2. Apache 1.3.x and 2.0.x

The probes in this section may be applied to instances of the Apache HTTP Server. Although the default values presume you will apply these probes using standard HTTP, you may also use them over secure connections by changing the application protocol to **`https`** and the port to **`443`**.

### C.2.1. Apache::Processes

The Apache::Processes probe monitors the processes executed on an Apache HTTP Server and collects the following metrics:

- Data Transferred Per Child — Records data transfer information only on individual children. A child process is one that is created from another process or the parent process.
- Data Transferred Per Slot — The cumulative amount of data transferred by a child process that restarts. The number of slots is configured in the `httpd.conf` file using the `MaxRequestsPerChild` setting.

The `ExtendedStatus` directive in the `httpd.conf` file of the Web server must be set to **`On`** for this probe to function properly.

| Field | Value |
|---|---|
| Application Protocol* | http |
| Port* | 80 |
| Pathname* | /server-status |
| UserAgent* | NOCpulse-ApacheUptime/1.0 |
| Username | |
| Password | |
| Timeout* | 15 |
| Critical Maximum Megabytes Transferred Per Child | |
| Warning Maximum Megabytes Transferred Per Child | |
| Critical Maximum Megabytes Transferred Per Slot | |
| Warning Maximum Megabytes Transferred Per Slot | |

**Table C-1. Apache::Processes settings**

### C.2.2. Apache::Traffic

The Apache::Traffic probe monitors the requests on an Apache HTTP Server and collects the following metrics:

- Current Requests — The number of requests being processed by the server at probe runtime.
- Request Rate — The events per second of accesses to the server since the probe last ran.
- Traffic — The kilobytes per second of traffic the server has processed since the probe last ran.

The `ExtendedStatus` directive in the `httpd.conf` file of the Web server must be set to **`On`** for this probe to function properly.

| Field | Value |
|---|---|
| Application Protocol* | http |
| Port* | 80 |
| Pathname* | /server-status |
| UserAgent* | NOCpulse-ApacheUptime/1.0 |
| Username | |
| Password | |
| Timeout* | 15 |
| Critical Maximum Current Requests (number) | |
| Warning Maximum Current Requests (number) | |
| Critical Maximum Request Rate (events per second) | |
| Warning Maximum Request Rate (events per second) | |
| Critical Maximum Traffic (kilobytes per second) | |
| Warning Maximum Traffic (kilobytes per second) | |

**Table C-2. Apache::Traffic settings**

### C.2.3. Apache::Uptime

The Apache::Uptime stores the cumulative time since the Web server was last started. No metrics are collected by this probe, which is designed to help track service level agreements (SLAs).

| Field | Value |
|---|---|
| Application Protocol* | http |
| Port* | 80 |
| Pathname* | /server-status |
| UserAgent* | NOCpulse-ApacheUptime/1.0 |
| Username | |
| Password | |
| Timeout* | 15 |

**Table C-3. Apache::Uptime settings**

## C.3. BEA WebLogic 6.x and higher

The probes in this section (with the exception of JDBC Connection Pool) can be configured to monitor the properties of any BEA WebLogic 6.x and higher server (Administration or Managed) running on a given host, even in a clustered environment. Monitoring of a cluster is achieved by sending all SNMP queries to the Administration Server of the domain and then querying its Managed Servers for individual data.

In order to obtain this higher level of granularity, the **BEA Domain Admin Server** parameter must be used to differentiate between the Administration Server receiving SNMP queries and the Managed Server undergoing the specified probe. If the host to be probed is the Administration Server, then the **BEA Domain Admin Server** parameter can be left blank, and both the SNMP queries and the probe will be sent to it only.

If the host to be probed is a Managed Server, then the IP address of the Administration Server should be provided in the **BEA Domain Admin Server** parameter, and the Managed Server name should be included in the **BEA Server Name** parameter and appended to the end of the **SNMP Community String** field. This causes the SNMP queries to be sent to the Administration Server host, as is required, but redirects the specific probe to the Managed Server host.

It should also be noted that the community string needed for probes run against Managed Server hosts should be in the form of **`community_prefix@managed_server_name`** in order for the SNMP query to return results for the desired Managed Server. Finally, SNMP must be enabled on each monitored system. SNMP support can be enabled and configured through the WebLogic Console.

Please see the documentation that came with your BEA server or information on the BEA website for more details about BEA's community string naming conventions: http://e-docs.bea.com/wls/docs70/snmpman/snmpagent.html

### C.3.1. BEA WebLogic::Execute Queue

The BEA WebLogic::Execute Queue probe monitors the WebLogic execute queue and provides the following metrics:

- Idle Execute Threads — The number of execution threads in an idle state.
- Queue Length — The number of requests in the queue.
- Request Rate — The number of requests per second.

This probe's transport protocol is User Datagram Protocol (UDP).

| Field | Value |
|---|---|
| SNMP Community String* | public |
| SNMP Port* | 161 |
| SNMP Version* | 1 |
| BEA Domain Admin Server | |
| BEA Server Name* | myserver |
| Queue Name* | default |
| Critical Maximum Idle Execute Threads | |
| Warning Maximum Idle Execute Threads | |
| Critical Maximum Queue Length | |
| Warning Maximum Queue Length | |
| Critical Maximum Request Rate | |
| Warning Maximum Request Rate | |

**Table C-4. BEA WebLogic::Execute Queue settings**

### C.3.2. BEA WebLogic::Heap Free

The BEA WebLogic::Heap Free probe collects the following metric:

- Heap Free — The percentage of free heap space.

This probe's transport protocol is User Datagram Protocol (UDP).

| Field | Value |
|---|---|
| SNMP Community String* | public |
| SNMP Port* | 161 |
| SNMP Version* | 1 |
| BEA Domain Admin Server | |
| BEA Server Name* | myserver |
| Critical Maximum Heap Free | |
| Warning Maximum Heap Free | |
| Warning Minimum Heap Free | |
| Critical Minimum Heap Free | |

**Table C-5. BEA WebLogic::Heap Free settings**

### C.3.3. BEA WebLogic::JDBC Connection Pool

The BEA WebLogic::JDBC Connection Pool probe monitors the Java Database Connection (JDBC) pool on a domain Admin Server only (no Managed Servers) and collects the following metrics:

- Connections — The number of connections to the JDBC.
- Connections Rate — The speed at which connections are made to the JDBC, measured in connections per second.
- Waiters — The number of sessions waiting to connect to the JDBC.

This probe's transport protocol is User Datagram Protocol (UDP).

| Field | Value |
|---|---|
| SNMP Community String* | public |
| SNMP Port* | 161 |
| SNMP Version* | 1 |
| BEA Domain Admin Server | |
| BEA Server Name* | myserver |
| JDBC Pool Name* | MyJDBC Connection Pool |
| Critical Maximum Connections | |
| Warning Maximum Connections | |

| Field | Value |
|---|---|
| Critical Maximum Connection Rate | |
| Warning Maximum Connection Rate | |
| Critical Maximum Waiters | |
| Warning Maximum Waiters | |

**Table C-6. BEA WebLogic::JDBC Connection Pool settings**

### C.3.4. BEA WebLogic::Server State

The BEA WebLogic::Server State probe monitors the current state of a BEA Weblogic Web server. If the probe is unable to make a connection to the server, a CRITICAL status results.

This probe's transport protocol is User Datagram Protocol (UDP).

| Field | Value |
|---|---|
| SNMP Community String* | public |
| SNMP Port* | 161 |
| SNMP Version* | 1 |
| BEA Domain Admin Server | |
| BEA Server Name* | |

**Table C-7. BEA WebLogic::Server State settings**

### C.3.5. BEA WebLogic::Servlet

The BEA WebLogic::Servlet probe monitors the performance of a particular servlet deployed on a WebLogic server and collects the following metrics:

- High Execution Time — The highest amount of time in milliseconds that the servlet takes to execute since the system was started.
- Low Execution Time — The lowest amount of time in milliseconds that the servlet takes to execute since the system was started.
- Execution Time Moving Average — A moving average of the execution time.
- Execution Time Average — A standard average of the execution time.
- Reload Rate — The number of times the specified servlet is reloaded per minute.
- Invocation Rate — The number of times the specified servlet is invoked per minute.

This probe's transport protocol is User Datagram Protocol (UDP).

| Field | Value |
|---|---|
| SNMP Community String* | public |
| SNMP Port* | 161 |

| Field | Value |
|---|---|
| SNMP Version* | 1 |
| BEA Domain Admin Server | |
| BEA Server Name* | myserver |
| Servlet Name* | |
| Critical Maximum High Execution Time | |
| Warning Maximum High Execution Time | |
| Critical Maximum Execution Time Moving Average | |
| Warning Maximum Execution Time Moving Average | |

**Table C-8. BEA WebLogic::Servlet settings**

## C.4. General

The probes in this section are designed to monitor basic aspects of your systems. When applying them, ensure their timed thresholds do not exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status will be returned in all instances of extended latency, thereby nullifying the thresholds.

### C.4.1. General::Remote Program

The General::Remote Program probe allows you to run any command or script on your system and obtain a status string. Note that the resulting message will be limited to 1024 bytes.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Command* | |
| OK Exit Status* | 0 |
| Warning Exit Status* | 1 |
| Critical Exit Status* | 2 |
| Timeout | 15 |

**Table C-9. General::Remote Program settings**

### C.4.2. General::Remote Program with Data

The General::Remote Program with Data probe allows you to run any command or script on your system and obtain a value, as well as a status string. To use this probe, you must include some XML code in the body of your script. This probe supports the following XML tags:

- <perldata> </perldata>
- <hash> </hash>

- <item key =" "> </item>

The remote program will need to output some iteration of the following code to `STDOUT`:

```
<perldata>
<hash>
<item key="data">10</item>
<item key="status_message">status message here</item>
</hash>
</perldata>
```

The required value for `data` is the data point to be inserted in the database for time-series trending. The `status_message` is optional and can be whatever text string is desired with a maximum length of 1024 bytes. Remote programs that do not include a `status_message` will still report the value and status returned.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe. XML is case-sensitive. The `data` item key name cannot be changed and it must collect a number as its value.

| Field | Value |
|---|---|
| Command* | |
| OK Exit Status* | 0 |
| Warning Exit Status* | 1 |
| Critical Exit Status* | 2 |
| Timeout | 15 |

**Table C-10. General::Remote Program with Data settings**

### C.4.3. General::SNMP Check

The General::SNMP Check probe tests your SNMP server by specifying a single object identifier (OID) in dotted notation (such as **`1.3.6.1.2.1.1.1.0`**) and a threshold associated with the return value. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the SNMP server to answer a connection request.

*Requirements* — SNMP must be running on the monitored system to perform this probe. Only integers can be used for the threshold values.

This probe's transport protocol is User Datagram Protocol (UDP).

| Field | Value |
|---|---|
| SNMP OID* | |
| SNMP Community String* | public |
| SNMP Port* | 161 |
| SNMP Version* | 2 |
| Timeout* | 15 |

| Field | Value |
|---|---|
| Critical Maximum Value | |
| Warning Maximum Value | |
| Warning Minimum Value | |
| Critical Minimum Value | |

**Table C-11. General::SNMP Check settings**

### C.4.4. General::TCP Check

The General::TCP Check probe tests your TCP server by verifying it can connect to a system via the specified port number. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the TCP server to answer a connection request.

The probe will pass the string specified in the **Send** field upon making a connection. The probe will anticipate a response from the system, which should include the substring specified in the **Expect** field. If the expected string is not found, the probe returns a CRITICAL status.

| Field | Value |
|---|---|
| Send | |
| Expect | |
| Port* | 1 |
| Timeout* | 10 |
| Critical Maximum Latency | |
| Warning Maximum Latency | |

**Table C-12. General::TCP Check settings**

### C.4.5. General::UDP Check

The General::UDP Check probe tests your UDP server by verifying it can connect to a system via the specified port number. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the UDP server to answer a connection request.

The probe will pass the string specified in the **Send** field upon making a connection. The probe will anticipate a response from the system, which should include the substring specified in the **Expect** field. If the expected string is not found, the probe returns a CRITICAL status.

This probe's transport protocol is User Datagram Protocol (UDP).

| Field | Value |
|---|---|
| Port* | 1 |

| Field | Value |
|---|---|
| Send | |
| Expect | |
| Timeout* | 10 |
| Critical Maximum Latency | |
| Warning Maximum Latency | |

**Table C-13. General::UDP Check settings**

### C.4.6. General::Uptime (SNMP)

The General::Uptime (SNMP) probe records the time since the device was last started. It uses the SNMP object identifier (OID) to obtain this value. The only error status it will return is UNKNOWN.

*Requirements* — SNMP must be running on the monitored system and access to the OID must be enabled to perform this probe.

This probe's transport protocol is User Datagram Protocol (UDP).

| Field | Value |
|---|---|
| SNMP Community String* | public |
| SNMP Port* | 161 |
| SNMP Version* | 2 |
| Timeout* | 15 |

**Table C-14. General::Uptime (SNMP) settings**

## C.5. Linux

The probes in this section monitor essential aspects of your Linux systems, from CPU usage to virtual memory. Apply them to mission-critical systems to obtain warnings prior to failure.

Unlike other probe groups, which may contain one or a few probes that require the Red Hat Network Monitoring Daemon, every Linux probe needs `rhnmd` to be running on the monitored system.

### C.5.1. Linux::CPU Usage

The Linux::CPU Usage probe monitors the CPU utilization on a system and collects the following metric:

- CPU Percent Used — The five-second average of the percent of CPU usage at probe execution.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to run this probe.

| Field | Value |
|---|---|

| Field | Value |
|---|---|
| Timeout* | 15 |
| Critical Maximum CPU Percent Used | |
| Warning Maximum CPU Percent Used | |

**Table C-15. Linux::CPU Usage settings**

### C.5.2. Linux::Disk IO Throughput

The Linux::Disk IO Throughput probe monitors a given disk and collects the following metric:

- Read Rate — The amount of data that is read in kilobytes per second.
- Write Rate — The amount of data that is written in kilobytes per second.

To obtain the value for the required **Disk number or disk name** field, run `iostat` on the system to be monitored and see what name has been assigned to the disk you desire. The default value of **0** will usually give you statistics from the first hard drive connected directly to the system.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe. Also, the **Disk number or disk name** parameter must match the format that is seen when the `iostat` command is run on the commandline. If the format is not identical, the configured probe will go into an UNKNOWN state.

| Field | Value |
|---|---|
| Disk number or disk name* | 0 |
| Timeout* | 15 |
| Critical Maximum KB read/second | |
| Warning Maximum KB read/second | |
| Warning Minimum KB read/second | |
| Critical Minimum KB read/second | |
| Critical Maximum KB written/second | |
| Warning Maximum KB written/second | |
| Warning Minimum KB written/second | |
| Critical Minimum KB written/second | |

**Table C-16. Linux::Disk IO Throughput settings**

### C.5.3. Linux::Disk Usage

The Linux::Disk Usage probe monitors the disk space on a specific file system and collects the following metrics:

- File System Used — The percentage of the file system currently in use.
- Space Used — The amount of the file system in megabytes currently in use.
- Space Available — The amount of the file system in megabytes currently available.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| File system* | /dev/hda1 |
| Timeout* | 15 |
| Critical Maximum File System Percent Used | |
| Warning Maximum File System Percent Used | |
| Critical Maximum Space Used | |
| Warning Maximum Space Used | |
| Warning Minimum Space Available | |
| Critical Minimum Space Available | |

**Table C-17. Linux::Disk Usage settings**

### C.5.4. Linux::Inodes

The Linux::Inodes probe monitors the specified file system and collects the following metric:

- Inodes — The percentage of inodes currently in use.

An inode is a data structure holding information about files in a Linux file system. There is an inode for each file, and a file is uniquely identified by the file system on which it resides and its inode number on that system.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| File system* | / |
| Timeout* | 15 |
| Critical Maximum Inodes Percent Used | |
| Warning Maximum Inodes Percent Used | |

**Table C-18. Linux::Inodes settings**

### C.5.5. Linux::Interface Traffic

The Linux::Interface Traffic probe measures the amount of traffic into and out of the specified interface (such as eth0) and collects the following metrics:

- Input Rate — The traffic in bytes per second going into the specified interface.
- Output Rate — The traffic in bytes per second going out of the specified interface.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Interface* | |
| Timeout* | 30 |
| Critical Maximum Input Rate | |
| Warning Maximum Input Rate | |
| Warning Minimum Input Rate | |
| Critical Minimum Input Rate | |
| Critical Maximum Output Rate | |
| Warning Maximum Output Rate | |
| Warning Minimum Output Rate | |
| Critical Minimum Output Rate | |

**Table C-19. Linux::Interface Traffic settings**

### C.5.6. Linux::Load

The Linux::Load probe monitors the CPU of a system and collects the following metric:

- Load — The average load on the system CPU over various periods.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Timeout* | 15 |
| Critical CPU Load 1-minute average | |
| Warning CPU Load 1-minute average | |
| Critical CPU Load 5-minute average | |
| Warning CPU Load 5-minute average | |
| Critical CPU Load 15-minute average | |
| Warning CPU Load 15-minute average | |

**Table C-20. Linux::Load settings**

### C.5.7. Linux::Memory Usage

The Linux::Memory Usage probe monitors the memory on a system and collects the following metric:

- RAM Free — The amount of free random access memory (RAM) in megabytes on a system.

You can also include the reclaimable memory in this metric by entering **`yes`** or **`no`** in the **Include reclaimable memory** field.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Include reclaimable memory | no |
| Timeout* | 15 |
| Warning Maximum RAM Free | |
| Critical Maximum RAM Free | |

**Table C-21. Linux::Memory Usage settings**

### C.5.8. Linux::Process Counts by State

The Linux::Process Counts by State probe identifies the number of processes in the following states:

- Blocked — One that has been switched to the waiting queue and the state of the process has been switched to the waiting state.
- Defunct — One that has terminated (either because it has been killed by a signal or because it has called `exit())` and whose parent process has not yet received notification of its termination by executing (some form of) the `wait()` system call.
- Stopped — One that has been stopped before its execution could be executed.
- Sleeping — One that is in the Interruptible sleep state that can later be reintroduced into memory and execution will resume where it left off.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Timeout* | 15 |
| Critical Maximum Blocked Processes | |
| Warning Maximum Blocked Processes | |
| Critical Maximum Defunct Processes | |
| Warning Maximum Defunct Processes | |
| Critical Maximum Stopped Processes | |
| Warning Maximum Stopped Processes | |
| Critical Maximum Sleeping Processes | |
| Warning Maximum Sleeping Processes | |
| Critical Maximum Child Processes | |
| Warning Maximum Child Processes | |

**Table C-22. Linux::Process Counts by State settings**

### C.5.9. Linux::Process Count Total

The Linux::Process Count Total probe monitors a system and collects the following metric:

- Process Count — The total number of processes currently running on the system.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Timeout* | 15 |
| Critical Maximum Process Count | |
| Warning Maximum Process Count | |

**Table C-23. Linux::Process Count Total settings**

### C.5.10. Linux::Process Health

The Linux::Process Health probe monitors user-specified processes and collects the following metrics:

- CPU Usage — The CPU usage rate for a given process in milliseconds per second. This metric reports the `time` column of `ps` output, which is the cumulative CPU time used by the process. This makes the metric independent of probe interval, allows sane thresholds to be set, and generates usable graphs (i.e. a sudden spike in CPU usage shows up as a spike in the graph).
- Child Process Groups — The number of child processes spawned from the specified parent process. A child process inherits most of its attributes, such as open files, from its parent.
- Threads — The number of running threads for a given process. A thread is the basic unit of CPU utilization, and consists of a program counter, a register set, and a stack space. A thread is also called a lightweight process.
- Physical Memory Used — The amount of physical memory (or RAM) in kilobytes being used by the specified process.
- Virtual Memory Used — The amount of virtual memory in kilobytes being used by the specified process, or the size of the process in real memory plus swap.

Specify the process by either command name or process I.D. (PID). Entering a PID will override the entry of a command name. If no command name or PID is entered, the error `Command not found` will be displayed and the probe will be set to a CRITICAL state.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Command Name | |
| Process ID (PID) file | |
| Timeout* | 15 |
| Critical Maximum CPU Usage | |
| Warning Maximum CPU Usage | |

| Field | Value |
|---|---|
| Critical Maximum Child Process Groups | |
| Warning Maximum Child Process Groups | |
| Critical Maximum Threads | |
| Warning Maximum Threads | |
| Critical Maximum Physical Memory Used | |
| Warning Maximum Physical Memory Used | |
| Critical Maximum Virtual Memory Used | |
| Warning Maximum Virtual Memory Used | |

**Table C-24. Linux::Process Health settings**

### C.5.11. Linux::Process Running

The Linux::Process Running probe verifies the specified process is functioning properly. It counts either processes or process groups, depending on whether the **Count process groups** checkbox is selected.

By default, the checkbox is selected, thereby indicating the probe should count the number of process group leaders independent of the number of children. This allows you, for example, to verify that two instances of the Apache HTTP Server are running regardless of the (dynamic) number of child processes. If it is not selected, the probe conducts a straightforward count of the number of processes (children and leaders) matching the specified process.

Specify the process by either command name or process I.D. (PID). Entering a PID will override the entry of a command name. If no command name or PID is entered, the error `Command not found` will be displayed and the probe will be set to a CRITICAL state.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Command name | |
| PID file | |
| Count process groups | (checked) |
| Timeout* | 15 |
| Critical Maximum Number Running | |
| Critical Minimum Number Running | |

**Table C-25. Linux::Process Running settings**

### C.5.12. Linux::Swap Usage

The Linux::Swap Usage probe monitors the swap partitions running on a system and reports the following metric:

- Swap Free — The percent of swap memory currently free.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Timeout* | 15 |
| Warning Minimum Swap Free | |
| Critical Minimum Swap Free | |

**Table C-26. Linux::Swap Usage settings**

### C.5.13. Linux::TCP Connections by State

The Linux::TCP Connections by State probe identifies the total number of TCP connections, as well as the quantity of each in the following states:

- TIME_WAIT — The socket is waiting after close for remote shutdown transmission so it may handle packets still in the network.
- CLOSE_WAIT — The remote side has been shut down and is now waiting for the socket to close.
- FIN_WAIT — The socket is closed, and the connection is now shutting down.
- ESTABLISHED — The socket has a connection established.
- SYN_RCVD — The connection request has been received from the network.

This probe can be helpful in finding and isolating network traffic to specific IP addresses or examining network connections into the monitored system.

The filter parameters for the probe let you narrow the probe's scope. This probe uses a command of `netstat -ant` to retrieve data. The **Local IP address** and **Local port** parameters use values in the **Local Address** column of the output; the **Remote IP address** and **Remote port** parameters use values in the **Foreign Address** column of the output for reporting.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Local IP address filter pattern list | |
| Local port number filter | |
| Remote IP address filter pattern list | |
| Remote port number filter | |
| Timeout* | 15 |
| Critical Maximum Total Connections | |
| Warning Maximum Total Connections | |
| Critical Maximum TIME_WAIT Connections | |
| Warning Maximum TIME_WAIT Connections | |

| Field | Value |
|---|---|
| Critical Maximum CLOSE_WAIT Connections | |
| Warning Maximum CLOSE_WAIT Connections | |
| Critical Maximum FIN_WAIT Connections | |
| Warning Maximum FIN_WAIT Connections | |
| Critical Maximum ESTABLISHED Connections | |
| Warning Maximum ESTABLISHED Connections | |
| Critical Maximum SYN_RCVD Connections | |
| Warning Maximum SYN_RCVD Connections | |

**Table C-27. Linux::TCP Connections by State settings**

### C.5.14. Linux::Users

The Linux::Users probe monitors the users of a system and reports the following metric:

- Users — The number of users currently logged in.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Timeout* | 15 |
| Critical Maximum Users | |
| Warning Maximum Users | |

**Table C-28. Linux::Users settings**

### C.5.15. Linux::Virtual Memory

The Linux::Virtual Memory probe monitors the total system memory and collects the following metric:

- Virtual Memory — The percent of total system memory - random access memory (RAM) plus swap - that is free.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| Timeout* | 15 |
| Warning Minimum Virtual Memory Free | |
| Critical Minimum Virtual Memory Free | |

**Table C-29. Linux::Virtual Memory settings**

## C.6. LogAgent

The probes in this section monitor the log files on your systems. You can use them to query logs for certain expressions and track the sizes of files. For LogAgent probes to run, the **nocpulse** user must be granted read access to your log files.

Note that data from the first run of these probes will not be measured against the thresholds to prevent spurious notifications caused by incomplete metric data. Measurements will begin on the second run.

### C.6.1. LogAgent::Log Pattern Match

The LogAgent::Log Pattern Match probe uses regular expressions to match text located within the log file being monitored and collects the following metrics:

- Regular Expression Matches — The number of matches that have occurred since the probe last ran.
- Regular Expression Match Rate — The number of matches per minute since the probe last ran.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe. For this probe to run, the **nocpulse** user must be granted read access to your log files.

In addition to the name and location of the log file to be monitored, you must provide a regular expression to be matched against in regex format for `egrep`, which is equivalent to `grep -E` in support for extended regular expressions. This is the regex set for `egrep`:

```
^ beginning of line
$ end of line
. match one char
* match zero or more chars
[] match one character set, e.g. '[Ff]oo'
[^] match not in set '[^A-F]oo'
+ match one or more of preceding chars
? match zero or one of preceding chars
| or, e.g. a|b
() groups chars, e.g., (foo|bar) or (foo)+
```

**Warning**

Do not include single quotation marks (') within the expression. Doing so will cause egrep to fail silently and the probe to time out.

| Field | Value |
|---|---|
| Log file* | /var/log/messages |
| Basic regular expression* | |
| Timeout* | 45 |
| Critical Maximum Matches | |
| Warning Maximum Matches | |
| Warning Minimum Matches | |
| Critical Minimum Matches | |

| Field | Value |
|---|---|
| Critical Maximum Match Rate | |
| Warning Maximum Match Rate | |
| Warning Minimum Match Rate | |
| Critical Maximum Match Rate | |

**Table C-30. LogAgent::Log Pattern Match settings**

### C.6.2. LogAgent::Log Size

The LogAgent::Log Size probe monitors log file growth and collects the following metrics:

- Size — The size the log file has grown in bytes since the probe last ran.
- Output Rate — The number of bytes per minute the log file has grown since the probe last ran.
- Lines — The number of lines written to the log file since the probe last ran.
- Line Rate — The number of lines written per minute to the log file since the probe last ran.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe. For this probe to run, the **`nocpulse`** user must be granted read access to your log files.

| Field | Value |
|---|---|
| Log file* | /var/log/messages |
| Timeout* | 20 |
| Critical Maximum Size | |
| Warning Maximum Size | |
| Warning Minimum Size | |
| Critical Minimum Size | |
| Critical Maximum Output Rate | |
| Warning Maximum Output Rate | |
| Warning Minimum Output Rate | |
| Critical Minimum Output Rate | |
| Critical Maximum Lines | |
| Warning Maximum Lines | |
| Warning Minimum Lines | |
| Critical Minimum Lines | |
| Critical Maximum Line Rate | |
| Warning Maximum Line Rate | |
| Warning Minimum Line Rate | |
| Critical Minimum Line Rate | |

Table C-31. LogAgent::Log Size settings

## C.7. MySQL 3.23 - 3.33

The probes in this section monitor aspects of the MySQL database using the `mysqladmin` binary. No specific user privileges are needed for these probes.

Note that the `mysql-server` package must be installed on the system conducting the monitoring for these probes to complete. Refer to the MySQL Installation section of the *RHN Satellite Server Installation Guide* for instructions.

### C.7.1. MySQL::Database Accessibility

The MySQL::Database Accessibility probe tests connectivity through a database account that has no database privileges. If no connection is made then a CRITICAL status results.

| Field | Value |
|---|---|
| Username* | |
| Password | |
| MySQL Port | 3306 |
| Database* | mysql |
| Timeout | 15 |

Table C-32. MySQL::Database Accessibility settings

### C.7.2. MySQL::Opened Tables

The MySQL::Opened Tables probe monitors the MySQL server and collects the following metric:

- Opened Tables — The tables that have been opened since the server was started.

| Field | Value |
|---|---|
| Username | |
| Password | |
| MySQL Port* | 3306 |
| Timeout | 15 |
| Critical Maximum Opened Objects | |
| Warning Maximum Opened Objects | |
| Warning Minimum Opened Objects | |
| Critical Minimum Opened Objects | |

Table C-33. MySQL::Opened Tables settings

### C.7.3. MySQL::Open Tables

The MySQL::Open Tables probe monitors the MySQL server and collects the following metric:

- Open Tables — The number of tables open when the probe runs.

| Field | Value |
|---|---|
| Username | |
| Password | |
| MySQL Port* | 3306 |
| Timeout | 15 |
| Critical Maximum Open Objects | |
| Warning Maximum Open Objects | |
| Warning Minimum Open Objects | |
| Critical Minimum Open Objects | |

**Table C-34. MySQL::Open Tables settings**

### C.7.4. MySQL::Query Rate

The MySQL::Query Rate probe monitors the MySQL server and collects the following metric:

- Query Rate — The average number of queries per second per database server.

| Field | Value |
|---|---|
| Username | |
| Password | |
| MySQL Port* | 3306 |
| Timeout | 15 |
| Critical Maximum Query Rate | |
| Warning Maximum Query Rate | |
| Warning Minimum Query Rate | |
| Critical Minimum Query Rate | |

**Table C-35. MySQL::Query Rate settings**

### C.7.5. MySQL::Threads Running

The MySQL::Threads Running probe monitors the MySQL server and collects the following metric:

- Threads Running — The total number of running threads within the database.

| Field | Value |
|---|---|
| Username | |
| Password | |
| MySQL Port* | 3306 |
| Timeout | 15 |
| Critical Maximum Threads Running | |
| Warning Maximum Threads Running | |
| Warning Minimum Threads Running | |
| Critical Minimum Threads Running | |

**Table C-36. MySQL::Threads Running settings**

## C.8. Network Services

The probes in this section monitor various services integral to a functioning network. When applying them, ensure their timed thresholds do not exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status will be returned in all instances of extended latency, thereby nullifying the thresholds.

### C.8.1. Network Services::DNS Lookup

The Network Services::DNS Lookup probe uses the `dig` command to see if it can resolve the system or domain name specified in the **Host or Address to look up** field. It collects the following metric:

- Query Time — The time in milliseconds required to execute the `dig` request.

This is useful in monitoring the status of your DNS servers. If you want to monitor one of your DNS servers, supply a well-known host/domain name, such as a large search engine or corporate Web site.

| Field | Value |
|---|---|
| Host or Address to look up | |
| Timeout* | 10 |
| Critical Maximum Query Time | |
| Warning Maximum Query Time | |

**Table C-37. Network Services::DNS Lookup settings**

### C.8.2. Network Services::FTP

The Network Services::FTP probe uses network sockets to test FTP port availability. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the FTP server to answer a connection request.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature.The optional **Expect** value is the string to be matched against after a successful connection is made to the FTP server. If the expected string is not found, the probe will return a CRITICAL state.

| Field | Value |
|---|---|
| Expect | FTP |
| Username | |
| Password | |
| FTP Port* | 21 |
| Timeout* | 10 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-38. Network Services::FTP settings**

### C.8.3. Network Services::IMAP Mail

The Network Services::IMAP Mail probe determines if it can connect to the IMAP 4 service on the system. Specifying an optional port will override the default port 143. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the IMAP server to answer a connection request.

The required **Expect** value is the string to be matched against after a successful connection is made to the IMAP server. If the expected string is not found, the probe will return a CRITICAL state.

| Field | Value |
|---|---|
| IMAP Port* | 143 |
| Expect* | OK |
| Timeout* | 5 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-39. Network Services::IMAP Mail settings**

### C.8.4. Network Services::Mail Transfer (SMTP)

The Network Services::Mail Transfer (SMTP) probe determines if it can connect to the SMTP port on the system. Specifying an optional port number will override the default port 25. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the SMTP server to answer a connection request.

| Field | Value |
|---|---|
| SMTP Port* | 25 |
| Timeout* | 10 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-40. Network Services::Mail Transfer (SMTP) settings**

### C.8.5. Network Services::Ping

The Network Services::Ping probe determines if the RHN Server can `ping` the monitored system or a specified IP address. It will also check the packet loss and compare the round trip average against the Warning and Critical threshold levels. The required **Packets to send** value allows you to control how many ICMP ECHO packets are sent to the system. This probe collects the following metrics:

- Round-Trip Average — The time it takes in milliseconds for the ICMP ECHO packet to go to and from the monitored system.
- Packet Loss — The percent of data lost in transit.

Although optional, the **IP Address** field can be instrumental in collecting metrics for systems that have multiple IP addresses. For instance, if the system is configured with multiple virtual IP addresses or uses Network Address Translation (NAT) to support internal and external IP addresses, this option may be used to check a secondary IP address, rather than the primary address associated with the hostname.

Note that this probe conducts the `ping` from an RHN Server and not the monitored system. So populating the IP Address field does not test connectivity between the system and the specified IP address but between the RHN Server and the IP address. Therefore, entering the same IP address for Ping probes on different systems accomplishes precisely the same task. To conduct a `ping` from a monitored system to an individual IP address, use the Remote Ping probe instead. Refer to Section C.8.7 *Network Services::Remote Ping*.

| Field | Value |
|---|---|
| IP Address (defaults to system IP) | |
| Packets to send* | 20 |
| Timeout* | 10 |
| Critical Maximum Round-Trip Average | |
| Warning Maximum Round-Trip Average | |
| Critical Maximum Packet Loss | |
| Warning Maximum Packet Loss | |

**Table C-41. Network Services::Ping settings**

### C.8.6. Network Services::POP Mail

The Network Services::POP Mail probe determines if it can connect to the POP3 port on the system. Specifying another port number (which is required) will override the default port 110. This probe

collects the following metric:

- Remote Service Latency — The time it takes in seconds for the POP server to answer a connection request.

The required **Expect** value is the string to be matched against after a successful connection is made to the POP server. The probe will look for the string in the first line of the response from the system. The default is **+OK**. If the expected string is not found, the probe will return a CRITICAL state.

| Field | Value |
|---|---|
| Port* | 110 |
| Expect* | +OK |
| Timeout* | 10 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-42. Network Services::POP Mail settings**

### C.8.7. Network Services::Remote Ping

The Network Services::Remote Ping probe determines if the monitored system can `ping` a specified IP address. It will also monitor the packet loss and compare the round trip average against the Warning and Critical threshold levels. The required **Packets to send** value allows you to control how many ICMP ECHO packets are sent to the address. This probe collects the following metrics:

- Round-Trip Average — The time it takes in milliseconds for the ICMP ECHO packet to go to and from the IP address.
- Packet Loss — The percent of data lost in transit.

The **IP Address** field identifies the precise address to be pinged. Unlike a similar field in the standard Ping probe that is optional, this field is required because the monitored system will be conducting the ping, rather than the RHN Server. Leaving this field blank within the standard Ping probe tells RHN to ping the primary address of the monitored system. Since the Remote Ping probe tests connectivity from the monitored system itself, another IP address must be specified. To conduct pings from the RHN Server to a system or IP address, use the standard Ping probe instead. Refer to Section C.8.5 *Network Services::Ping*.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe.

| Field | Value |
|---|---|
| IP Address* | |
| Packets to send* | 20 |
| Timeout* | 10 |
| Critical Maximum Round-Trip Average | |
| Warning Maximum Round-Trip Average | |
| Critical Maximum Packet Loss | |

| Field | Value |
|---|---|
| Warning Maximum Packet Loss | |

**Table C-43. Network Services::Remote Ping settings**

### C.8.8. Network Services::RPCService

The Network Services::RPCService probe tests the availability of remote procedure call (RPC) programs on a given IP address. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the RPC server to answer a connection request.

RPC server programs (which provide function calls via that RPC network) register themselves in the RPC network by declaring a program ID and a program name. NFS is an example of a service that works via the RPC mechanism.

Client programs that wish to use the resources of RPC server programs do so by asking the machine on which the server program resides to provide access to RPC functions within the RPC program number or program name. These conversations can occur over either TCP or UDP (but are almost always UDP).

This probe lets you test simple program availability. You will need to specify the program name or program number and the protocol over which the conversation will occur (plus the usual timeout).

| Field | Value |
|---|---|
| Protocol (TCP/UDP) | udp |
| Service Name* | nfs |
| Timeout* | 10 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-44. Network Services::RPCService settings**

### C.8.9. Network Services::Secure Web Server (HTTPS)

The Network Services::Secure Web Server (HTTPS) probe determines the availability of the secure Web server and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the HTTPS server to answer a connection request.

This probe confirms it can connect to the HTTPS port on the specified host and retrieve the specified URL. If no URL is specified, the probe will fetch the root document. The probe looks for a HTTP/1. message from the system, unless you alter that value. Specifying another port number will override the default port of 443.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature. Unlike most other probes, this probe will return a CRITICAL status if it cannot contact the system within the timeout period.

| Field | Value |
|---|---|
| URL Path | / |
| Expect Header | HTTP/1 |
| Expect Content | |
| UserAgent* | NOCpulse-check_http/1.0 |
| Username | |
| Password | |
| Timeout* | 10 |
| HTTPS Port* | 443 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-45. Network Services::Secure Web Server (HTTPS) settings**

### C.8.10. Network Services::SSH

The Network Services::SSH probe determines the availability of SSH on the specified port and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the SSH server to answer a connection request.

Upon successfully contacting the SSH server and receiving a valid response, the probe will display the protocol and server version information. If the probe receives an invalid response, it will display the message returned from the server and generate a WARNING state.

| Field | Value |
|---|---|
| SSH Port* | 22 |
| Timeout* | 5 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-46. Network Services::SSH settings**

### C.8.11. Network Services::Web Server (HTTP)

The Network Services::Web Server (HTTP) probe determines the availability of the Web server and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the HTTP server to answer a connection request.

This probe confirms it can connect to the HTTP port on the specified host and retrieve the specified URL. If no URL is specified, the probe will fetch the root document. The probe looks for a HTTP/1. message from the system, unless you alter that value. Specifying another port number will override

the default port of 80. Unlike most other probes, this probe will return a CRITICAL status if it cannot contact the system within the timeout period.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature. Also, the optional Virtual Host field can be used to monitor a separate documentation set located on the same physical machine presented as a standalone server. If your Web server is not configured to use virtual hosts (which is typically the case), you should leave this field blank. If you do have virtual hosts configured, enter the domain name of the first host here. Add as many probes as necessary to monitor all virtual hosts on the machine.

| Field | Value |
|---|---|
| URL Path | / |
| Virtual Host | |
| Expect Header | HTTP/1 |
| Expect Content | |
| UserAgent* | NOCpulse-check_http/1.0 |
| Username | |
| Password | |
| Timeout* | 10 |
| HTTP Port* | 80 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-47. Network Services::Web Server (HTTP) settings**

## C.9. Oracle 8i and 9i

The probes in this section may be applied to instances of the Oracle database matching the versions supported. Oracle probes require the configuration of the database and associations made by running: `$ORACLE_HOME/rdbms/admin/catalog.sql` In addition, for these probes to function properly, the Oracle user configured in the probe must have minimum privileges of CONNECT and SELECT_CATALOG_ROLE.

Some Oracle probes are specifically aimed at tuning devices for long-term performance gains, rather than avoiding outages. Therefore, Red Hat recommends scheduling them to occur less frequently, between every hour and every two days. This will provide a better statistical representation than every few minutes while de-emphasizing anomalies that can occur. This applies to following probes: Buffer Cache, Data Dictionary Cache, Disk Sort Ratio, Library Cache, and Redo Log.

For CRITICAL and WARNING thresholds based upon time to work as intended, their values cannot exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status will be returned in all cases of extended latency, thereby nullifying the thresholds. For this reason, Red Hat strongly recommends ensuring timeout periods exceed all timed thresholds. In this section, this refers specifically to the probe TNS Ping.

Finally, customers using these Oracle probes against a database using Oracle's Multi-Threaded Server (MTS) will need to contact Red Hat support to have entries added to the RHN Server's /etc/hosts file to ensure the DNS name is resolved correctly.

### C.9.1. Oracle::Active Sessions

The Oracle::Active Sessions probe monitors an Oracle instance and collects the following metrics:

- Active Sessions — The number of active sessions based on the value of `V$PARAMETER.PROCESSES`.
- Available Sessions — The percentage of active sessions based on the value of `V$PARAMETER.PROCESSES`.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Timeout* | 30 |
| Critical Maximum Active Sessions | |
| Warning Maximum Active Sessions | |
| Critical Maximum Available Sessions Used | |
| Warning Maximum Available Sessions Used | |

**Table C-48. Oracle::Active Sessions settings**

### C.9.2. Oracle::Availability

The Oracle::Availability probe determines the availability of the database from the RHN Satellite Server.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Timeout* | 30 |

**Table C-49. Oracle::Availability settings**

### C.9.3. Oracle::Blocking Sessions

The Oracle::Blocking Sessions probe monitors an Oracle instance and collects the following metric:

- Blocking Sessions — The number of sessions preventing other sessions from committing changes to the Oracle database, as determined by the required *Time Blocking* value provided by you. Only those sessions that have been blocking for this duration, which is measured in seconds, will be counted as blocking sessions.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Time Blocking (seconds)* | 20 |
| Timeout* | 30 |
| Critical Maximum Blocking Sessions | |
| Warning Maximum Blocking Sessions | |

**Table C-50. Oracle::Blocking Sessions settings**

### C.9.4. Oracle::Buffer Cache

The Oracle::Buffer Cache probe computes the Buffer Cache Hit Ratio so as to optimize the system global area (SGA) Database Buffer Cache size. It collects the following metrics:

- Db Block Gets — The number of blocks accessed via single block gets (not through the consistent get mechanism).
- Consistent Gets — The number of accesses made to the block buffer to retrieve data in a consistent mode.
- Physical Reads — The cumulative number of blocks read from disk.
- Buffer Cache Hit Ratio — The rate the database goes to the buffer instead of the hard disk to retrieve data. A low ratio suggests more RAM should be added to the system.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port | 1521 |
| Timeout* | 30 |
| Warning Minimum Buffer Cache Hit Ratio | |
| Critical Minimum Buffer Cache Hit Ratio | |

**Table C-51. Oracle::Buffer Cache settings**

### C.9.5. Oracle::Client Connectivity

The Oracle::Client Connectivity probe determines if the database is up and capable of receiving connections from the monitored system. This probe opens an `rhnmd` connection to the system and issues a `sqlplus connect` command to be run on the same monitored system.

The **Expected DB name** parameter is the expected value of `V$DATABASE.NAME`. This value is case-

insensitive. A CRITICAL status is returned if this value is not found.

*Requirements* — The Red Hat Network Monitoring Daemon (`rhnmd`) must be running on the monitored system to execute this probe. For this probe to run, the **`nocpulse`** user must be granted read access to your log files.

| Field | Value |
|---|---|
| Oracle Hostname or IP address* | |
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| ORACLE_HOME* | /opt/oracle |
| Expected DB Name* | |
| Timeout* | 30 |

**Table C-52. Oracle::Client Connectivity settings**

### C.9.6. Oracle::Data Dictionary Cache

The Oracle::Data Dictionary Cache probe computes the Data Dictionary Cache Hit Ratio so as to optimize the SHARED_POOL_SIZE in `init.ora`. It collects the following metrics:

- Data Dictionary Hit Ratio — The ratio of cache hits to cache lookup attempts in the data dictionary cache. In other words, the rate the database goes to the dictionary instead of the hard disk to retrieve data. A low ratio suggests more RAM should be added to the system.
- Gets — The number of blocks accessed via single block gets (not through the consistent get mechanism).
- Cache Misses — The number of accesses made to the block buffer to retrieve data in a consistent mode.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Timeout* | 30 |
| Warning Minimum Data Dictionary Hit Ratio | |
| Critical Minimum Data Dictionary Hit Ratio | |

**Table C-53. Oracle::Data Dictionary Cache settings**

### C.9.7. Oracle::Disk Sort Ratio

The Oracle::Disk Sort Ratio probe monitors an Oracle database instance and collects the following metric:

- Disk Sort Ratio — The rate of Oracle sorts that were too large to be completed in memory and were instead sorted using a temporary segment.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Timeout* | 30 |
| Critical Maximum Disk Sort Ratio | |
| Warning Maximum Disk Sort Ratio | |

**Table C-54. Oracle::Disk Sort Ratio settings**

### C.9.8. Oracle::Idle Sessions

The Oracle::Idle Sessions probe monitors an Oracle instance and collects the following metric:

- Idle Sessions — The number of Oracle sessions that are idle, as determined by the required *Time Idle* value provided by you. Only those sessions that have been idle for this duration, which is measured in seconds, will be counted as idle sessions.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Time Idle (seconds)* | 20 |
| Timeout* | 30 |
| Critical Maximum Idle Sessions | |
| Warning Maximum Idle Sessions | |

**Table C-55. Oracle::Idle Sessions settings**

### C.9.9. Oracle::Index Extents

The Oracle::Index Extents probe monitors an Oracle instance and collects the following metric:

- Allocated Extents — The number of allocated extents for any index.
- Available Extents — The percentage of available extents for any index.

The required **Index Name** field contains a default value of `%` that will match any index name.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Index Owner* | % |
| Index Name* | % |
| Timeout* | 30 |
| Critical Maximum of Allocated Extents | |
| Warning Maximum of Allocated Extents | |
| Critical Maximum of Available Extents | |
| Warning Maximum of Available Extents | |

**Table C-56. Oracle::Index Extents settings**

### C.9.10. Oracle::Library Cache

The Oracle::Library Cache probe computes the Library Cache Miss Ratio so as to optimize the SHARED_POOL_SIZE in `init.ora`. It collects the following metrics:

- Library Cache Miss Ratio — The rate a library cache pin miss occurs. This will happen when a session executes a statement that it has already parsed but finds that the statement is no longer in the shared pool.
- Executions — The number of times a pin was requested for objects of this namespace.
- Cache Misses — The number of pins of objects with previous pins since the object handle was created that must now retrieve the object from disk.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Timeout* | 30 |
| Critical Maximum Library Cache Miss Ratio | |
| Warning Maximum Library Cache Miss Ratio | |

**Table C-57. Oracle::Library Cache settings**

### C.9.11. Oracle::Locks

The Oracle::Locks probe monitors an Oracle database instance and collects the following metric:

- Active Locks — The current number of active locks as determined by the value in the v$locks table. Database administrators should be aware of high numbers of locks present in a database instance.

Locks are used so that multiple users or processes updating the same data in the database do not conflict. This probe is useful for alerting database administrators when a high number of locks are present in a given instance.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Timeout* | 30 |
| Critical Maximum Active Locks | |
| Warning Maximum Active Locks | |

**Table C-58. Oracle::Locks settings**

### C.9.12. Oracle::Redo Log

The Oracle::Redo Log probe monitors an Oracle database instance and collects the following metrics:

- Redo Log Space Request Rate — The average number of redo log space requests per minute since the server has been started.
- Redo Buffer Allocation Retry Rate — The average number of buffer allocation retries per minute since the server was started.

The metrics returned and the thresholds they're measured against are numbers representing the rate of change in events per minute. The rate of change for these metrics should be monitored because fast growth can indicate problems requiring investigation.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Timeout* | 30 |
| Critical Maximum Redo Log Space Request Rate | |
| Warning Maximum Redo Log Space Request Rate | |

| Field | Value |
|---|---|
| Critical Maximum Redo Buffer Allocation Retry Rate | |
| Warning Maximum Redo Buffer Allocation Retry Rate | |

**Table C-59. Oracle::Redo Log settings**

### C.9.13. Oracle::Table Extents

The Oracle::Table Extents probe monitors an Oracle database instance and collects the following metrics:

- Allocated Extents-Any Table — The total number of extents for any table.
- Available Extents-Any Table — The percentage of available extents for any table.

In Oracle, table extents are how a table grows. When a table is full, it is *extended* by an amount of space configured when the table is created. Extents are configured on a per-table basis, with an extent size and a maximum number of extents.

For example, a table that starts with 10 MB of space and is configured with an extent size of 1 MB and max extents of 10 can grow to a maximum of 20 MB (by being extended by 1 MB ten times). This probe can be configured to alert by (1) the number of allocated extents (e.g. "go critical when the table has been extended 5 or more times"), or (2) the table is extended past a certain percentage of its max extents (e.g. "go critical when the table has exhausted 80% or more of its max extents").

The required **Table Owner** and **Table Name** fields contain a default value of `%` that will match any table owner or name.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Table Owner* | % |
| Table Name* | % |
| Timeout* | 30 |
| Critical Maximum Allocated Extents | |
| Warning Maximum Allocated Extents | |
| Critical Maximum Available Extents | |
| Warning Maximum Available Extents | |

**Table C-60. Oracle::Table Extents settings**

### C.9.14. Oracle::Tablespace Usage

The Oracle::Tablespace Usage probe monitors an Oracle database instance and collects the following

metric:

- Available Space Used — The percentage of available space in each tablespace that has been used.

Tablespace is the shared pool of space in which a set of tables live. This probe alerts the user when the total amount of available space falls below the threshold. Tablespace is measured in bytes, so extents don't factor into it directly (though each extension removes available space from the shared pool).

The required **Tablespace Name** field is case insensitive and contains a default value of `%` that will match any table name.

| Field | Value |
|---|---|
| Oracle SID* | |
| Oracle Username* | |
| Oracle Password* | |
| Oracle Port* | 1521 |
| Tablespace Name* | % |
| Timeout* | 30 |
| Critical Maximum Available Space Used | |
| Warning Maximum Available Space Used | |

**Table C-61. Oracle::Tablespace Usage settings**

### C.9.15. Oracle::TNS Ping

The Oracle::TNS Ping determines if an Oracle listener is alive and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the Oracle server to answer a connection request.

| Field | Value |
|---|---|
| TNS Listener Port* | 1521 |
| Timeout* | 15 |
| Critical Maximum Remote Service Latency | |
| Warning Maximum Remote Service Latency | |

**Table C-62. Oracle::TNS Ping settings**

## C.10. RHN Satellite Server

The probes in this section may be applied to the RHN Satellite Server itself to monitor its health and performance. Since these probes run locally, no specific application or transport protocols are required.

### C.10.1. RHN Satellite Server::Disk Space

The RHN Satellite Server::Disk Space probe monitors the free disk space on a Satellite and collects the following metrics:

- File System Used — The percent of the current filesystem now in use.
- Space Used — The file size used by the current filesystem.
- Space Available — The file size available to the current filesystem.

| Field | Value |
|---|---|
| Device Pathname* | /dev/hda1 |
| Critical Maximum File System Used | |
| Warning Maximum File System Used | |
| Critical Maximum Space Used | |
| Warning Maximum Space Used | |
| Critical Maximum Space Available | |
| Warning Maximum Space Available | |

**Table C-63. RHN Satellite Server::Disk Space settings**

### C.10.2. RHN Satellite Server::Execution Time

The RHN Satellite Server::Execution Time probe monitors the execution time for probes run from a Satellite and collects the following metric:

- Probe Execution Time Average — The seconds it takes to fully execute a probe.

| Field | Value |
|---|---|
| Critical Maximum Probe Execution Time Average | |
| Warning Maximum Probe Execution Time Average | |

**Table C-64. RHN Satellite Server::Execution Time settings**

### C.10.3. RHN Satellite Server::Interface Traffic

The RHN Satellite Server::Interface Traffic probe monitors the interface traffic on a Satellite and collects the following metrics:

- Input Rate — The amount of traffic in bytes per second the device receives.
- Output Rate — The amount of traffic in bytes per second the device sends.

| Field | Value |
|---|---|
| Interface* | eth0 |

| Field | Value |
|---|---|
| Timeout (seconds)* | 30 |
| Critical Maximum Input Rate | |
| Critical Maximum Output Rate | |

**Table C-65. RHN Satellite Server::Interface Traffic settings**

### C.10.4. RHN Satellite Server::Latency

The RHN Satellite Server::Latency probe monitors the latency of probes on a Satellite and collects the following metric:

- Probe Latency Average — The lag in seconds between the time a probe becomes ready to run and the time it is actually run. Under normal conditions, this will generally be less than a second. When a Satellite is overloaded (because it has too many probes with respect to their average execution time), the number goes up.

| Field | Value |
|---|---|
| Critical Maximum Probe Latency Average | |
| Warning Maximum Probe Latency Average | |

**Table C-66. RHN Satellite Server::Latency settings**

### C.10.5. RHN Satellite Server::Load

The RHN Satellite Server::Load probe monitors the CPU load on a Satellite and collects the following metric:

- Load — The load average on the CPU for a 1-, 5-, and 15-minute period.

| Field | Value |
|---|---|
| Critical Maximum 1-minute Average | |
| Warning Maximum 1-minute Average | |
| Critical Maximum 5-minute Average | |
| Warning Maximum 5-minute Average | |
| Critical Maximum 15-minute Average | |
| Warning Maximum 15-minute Average | |

**Table C-67. RHN Satellite Server::Load settings**

### C.10.6. RHN Satellite Server::Probe Count

The RHN Satellite Server::Probe Count probe monitors the number of probes on a Satellite and collects the following metric:

- Probes — The number of individual probes running on a Satellite.

| Field | Value |
|---|---|
| Critical Maximum Probe Count | |
| Warning Maximum Probe Count | |

**Table C-68. RHN Satellite Server::Probe Count settings**

### C.10.7. RHN Satellite Server::Process Counts

The RHN Satellite Server::Process Counts probe monitors the number of processes on a Satellite and collects the following metrics:

- Blocked — The number of processes that have been switched to the waiting queue and waiting state.
- Child — The number of processes spawned by another process already running on the machine.
- Defunct — The number of processes that have terminated (either because they have been killed by a signal or have called `exit()`) and whose parent processes have not yet received notification of their termination by executing (some form of) the `wait()` system call.
- Stopped — The number of processes that have been stopped before their executions could be completed.
- Swapped — The number of processes that have been written to disk, generally due to a severe memory shortfall.

| Field | Value |
|---|---|
| Critical Maximum Blocked Processes | |
| Warning Maximum Blocked Processes | |
| Critical Maximum Child Processes | |
| Warning Maximum Child Processes | |
| Critical Maximum Defunct Processes | |
| Warning Maximum Defunct Processes | |
| Critical Maximum Stopped Processes | |
| Warning Maximum Stopped Processes | |
| Critical Maximum Swapped Processes | |
| Warning Maximum Swapped Processes | |

**Table C-69. RHN Satellite Server::Process Counts settings**

### C.10.8. RHN Satellite Server::Processes

The RHN Satellite Server::Processes probe monitors the number of processes on a Satellite and collects the following metric:

- Processes — The number of processes running simultaneously on the machine.

| Field | Value |
|---|---|
| Critical Maximum Processes | |
| Warning Maximum Processes | |

**Table C-70. RHN Satellite Server::Processes settings**

### C.10.9. RHN Satellite Server::Process Health

The RHN Satellite Server::Process Health probe monitors customer-specified processes and collects the following metrics:

- CPU Usage — The CPU usage percent for a given process.
- Child Process Groups — The number of child processes spawned from the specified parent process. A child process inherits most of its attributes, such as open files, from its parent.
- Threads — The number of running threads for a given process. A thread is the basic unit of CPU utilization, and consists of a program counter, a register set, and a stack space. A thread is also called a lightweight process.
- Physical Memory Used — The amount of physical memory in kilobytes being used by the specified process.
- Virtual Memory Used — The amount of virtual memory in kilobytes being used by the specified process, or the size of the process in real memory plus swap.

Specify the process by either command name or process I.D. (PID). Entering a PID will override the entry of a command name. If no command name or PID is entered, the error `Command not found` will be displayed and the probe will be set to a CRITICAL state.

| Field | Value |
|---|---|
| Command Name | |
| Process ID (PID) file | |
| Timeout* | 15 |
| Critical Maximum CPU Usage | |
| Warning Maximum CPU Usage | |
| Critical Maximum Child Process Groups | |
| Warning Maximum Child Process Groups | |
| Critical Maximum Threads | |
| Warning Maximum Threads | |
| Critical Maximum Physical Memory Used | |
| Warning Maximum Physical Memory Used | |
| Critical Maximum Virtual Memory Used | |
| Warning Maximum Virtual Memory Used | |

**Table C-71. RHN Satellite Server::Process Health settings**

### C.10.10. RHN Satellite Server::Process Running

The RHN Satellite Server::Process Running probe verifies that the specified process is running. Specify the process by either command name or process I.D. (PID). Entering a PID will override the entry of a command name. A Critical status results if the probe cannot verify the command or PID.

| Field | Value |
|---|---|
| Command Name | |
| Process ID (PID) file | |
| Critical Number Running Maximum | |
| Critical Number Running Minimum | |

**Table C-72. RHN Satellite Server::Process Running settings**

### C.10.11. RHN Satellite Server::Swap

The RHN Satellite Server::Swap probe monitors the percent of free swap space available on a Satellite. A CRITICAL status results if the value falls below the Critical threshold. A WARNING status results if the value falls below the Warning threshold.

| Field | Value |
|---|---|
| Critical Minimum Swap Percent Free | |
| Warning Minimum Swap Percent Free | |

**Table C-73. RHN Satellite Server::Swap settings**

### C.10.12. RHN Satellite Server::Users

The RHN Satellite Server::Users probe monitors the number of users currently logged into a Satellite. A CRITICAL status results if the value exceeds the Critical threshold. A WARNING status results if the value exceeds the Warning threshold.

| Field | Value |
|---|---|
| Critical Maximum Users | |
| Warning Maximum Users | |

**Table C-74. RHN Satellite Server::Users settings**

# Glossary

## A

### Action

A task that is scheduled by a system administrator using Red Hat Network to be performed on one or more client systems. For example, an action can be scheduled to update the kernel packages on all the systems within a selected group.

### Activation Key

RHN Management and Provisioning customers can generate activation keys through the RHN website. Each unique key can then be used to register a Red Hat system, entitle the system to RHN, subscribe the system to specific channels, and subscribe the system to RHN system groups through the command line utility `rhnreg_ks` from the `rhn_register` package.

## B

### Base Channel

A base channel is a type of *Channel* that consists of a list of packages based on a specific architecture and Red Hat release. For example, all the packages in Red Hat Enterprise Linux AS 3 for the x86 architecture make a base channel.

### Bug Fix Alert

An *Errata Alert* that pertains to a bug fix.

### Bugzilla

Bugzilla is an online application (http://www.redhat.com/bugzilla) that allows users to communicate directly with the developers. From Bugzilla, users can submit bug reports and feature requests for Red Hat Enterprise Linux and related open source packages.

## C

### Channel

A channel is a list of packages. Channels are used to choose packages to be installed from client systems. Every client system must be subscribed to one *Base Channel* and can be subscribed to one or more *Child Channel* .

### Child Channel

A child channel is a *Channel* associated with a *Base Channel* but contains extra packages.

### Client System

See *Registered System* .

## D

### Digital Certificate

A client component in XML format that is stored in the `/etc/sysconfig/rhn/systemid` file on registered systems. Red Hat Network verifies this certificate to authenticate the registered system before each connection. This certificate is issued by Red Hat and passed to the system as part of the registration process. It includes unique information about the registered system to avoid fraudulent use.

## E

### Email Notification

Similar to an *Errata Alert* , except the information is delivered via email. If the email notifications option is selected, notifications are sent for every Red Hat Network *Errata Alert* . The email includes the type of Errata Alert, summary of the Errata, description of the Errata, and a list of which systems are affected by the report.

### Enhancement Alert

An *Errata Alert* that pertains to a package enhancement request.

### Entitled Server

A server that is subscribed to an RHN service level. Because the server is entitled, the RHN website can be used to manage its packages.

### Errata

Information published by Red Hat describing security fixes, bug fixes, and package enhancements for Red Hat Enterprise Linux. The information includes the topics of the Errata, Bugzilla bug IDs, relevant releases/architectures, solutions including required RPMs, and MD5 checksums for verification. Errata are also available at http://www.redhat.com/errata/. Each RHN *Errata Alert* is based on the Red Hat Enterprise Linux Errata List.

Security issues and bug fixes are submitted by Red Hat engineers as well as the Linux community through Bugzilla which generates a bug report for each issue. Red Hat engineering evaluates the reports, resolves the bug, and generates new RPM packages. After the Red Hat quality assurance

team tests new packages they are placed on the Red Hat Public File Server and on the Red Hat Network Server and an Errata is generated.

### Errata Alert

RHN Errata Alert that updated packages based on Red Hat Errata are available for one or more systems within an organization. There are three types of Errata Alerts: Security Alerts, Bug Fix Alerts, and Enhancement Alerts.

## M

### Management

One of the RHN service level offerings. It has more features than the Update service level, including user management, system groups, and enhanced system details.

## O

### Organization Administrator

Organization Administrator are sets of users that have the highest level of control over an organization's Red Hat Network account. Members of this group can add users, systems, and system groups to the organization as well as remove them. An Organization Administrator can also give users administrative privileges to system groups. An RHN organization must have at least one member of the Organization Administrator group.

## P

### Package

All software in Red Hat Enterprise Linux is divided into software packages. Software updates are released in the form of RPM packages that can be installed on a Red Hat Enterprise Linux system.

### Provisioning

One of the RHN service level offerings. It has more features than the Management service level, including kickstarting, reconfiguring, tracking, and reverting systems.

# R

### Registered System

A system that is registered with Red Hat Network. Also known as a client system.

### Red Hat Network Daemon

The RHN client daemon (`rhnsd`) that periodically polls Red Hat Network for scheduled actions.

### Red Hat Network Registration Client

The RHN client application (`rhn_register`) that collects information about the client system, creates a *System Profile* and *Digital Certificate* , establishes a connection with the Red Hat Network servers, and registers the system with Red Hat Network.

### Red Hat Update Agent

The RHN client application (`up2date`) that allows users to retrieve and install all updated packages for the client system on which the application is run. Use the **Red Hat Update Agent Configuration Tool** to configure its preferences, including whether to install the packages after they are downloaded.

### RPM

A software package manager that was developed by Red Hat. It can be used to build, install, query, verify, update, and uninstall software packages. All software updates from RHN are delivered in RPM format.

### RPM Database

Each Red Hat Enterprise Linux system has an RPM database that stores information about all the RPM packages installed on the system. This information includes the version of the package, which files were installed with the package, a brief description of the package, the installation date, and more.

### RPM Update

Red Hat Network option to deliver the RPM packages based on the *Errata Alert* list to a client system without user intervention. If this feature is selected, packages are delivered through the *Red Hat Network Daemon* running on the client system.

# S

### Security Alert

An *Errata Alert* that pertains to system security.

### Service Level

A Red Hat Network subscription service. Different service levels offer different features of RHN. There are three paid service levels currently available: RHN Update, RHN Management, and RHN Provisioning.

### Software Manager

The name of the first *Service Level* offering for Red Hat Network. Software Manager is now known as RHN *Update* .

### System Directory

The System Directory section of Red Hat Network allows an organization to divide its client systems into system groups. Only members of the *Organization Administrator* group can add systems to the organization.

### System ID

A unique string of characters and numbers that identifies a registered system. It is stored in the system's *Digital Certificate* .

### System Profile

Hardware and software information about the client system. It is created during the registration process. The software information is a list of RPM packages and their versions installed on the client system. The System Profile is used to determine every *Errata Alert* relevant to each client system.

### System Set Manager

Interface that allows users to perform actions on multiple systems. Actions include applying Errata Updates, upgrading packages, and adding/removing systems to/from system groups.

## U

### Update

One of the RHN service level offerings. Update was formerly called Basic. Update offers the same services as the Basic subscription did, plus more new features.

# Index


## A

account
  deactivate, 62
action
  completed systems, 111
  details, 111
  failed systems, 111
  in progress systems, 111
activation key, 85
  deleting, 86
  disabling, 86
  editing, 86
activation keys
  creating, editing, and deleting, 85
  multiple use, 86
  registration, 34
  using, 35
addresses
  change, 62
Apache
  probes, 142
  Processes, 142
  Traffic, 142
  Uptime, 143
application programming interface
  API, 137

## B

base channel, 97

## C

changing email address, 114
changing password, 114
Channel Entitlements, 101
Channel List, 97
channels, 97
  all, 99
  base, 97
  child, 97
  entitling, 101
  errata, 100
  list of, 97
  packages, 100
  relevant, 98
  retired, 99
  Software and Configuration Files, 97
Channels and Packages
  Channel List, 97
child channel, 97
client applications
  obtaining, 5
Config Channel List, 104
config channels
  details, 106, 107
  global, 105
  list of, 104
Config Channels and Files
  Config Channel List, 104
config management
  system preparation, 104
Configuration
  Channel List
    Channel Details, 106
    File Details, 107
configuration files
  manage, 105
  quota, 105
Configuration Management
  command line tools, 129
conventions
  document, i
custom information
  about systems, 69

## D

daemon, 37
deleting a system, 68
Demo
  service level, 2
Digital Certificate, 4
download ISO images, 101

## E

email address
  change, 62
  changing, 114
entitlement
  with activation key, 85
entitlements
  purchase history, 63
Errata, 94
  Advanced Search, 97
  All Errata, 96
  apply applicable, 70
  Relevant Errata, 95
Errata Alert Icons
  explanation of, 59
Errata Alerts
  applying, 96
  searching, 97
  viewing details, 97
  viewing list of all errata, 96

viewing list of applicable errata, 95
Errata notifications
automatic updates, 4

## G

General
probes, 147
Remote Program, 147
Remote Program with Data, 147
SNMP Check, 148
TCP Check, 149
UDP Check, 149
Uptime (SNMP), 150
getting started, 5
GNU Privacy Guard, 5

## H

hardware profile
Updating on server, 69
Help Desk, 63

## I

ISO images
all, 101
download, 101
relevant, 101

## K

kickstart
explained, 88
prerequisites, 88
kickstart details
page and tabs, 89
kickstart profiles
creating, 89

## L

Linux
CPU Usage, 150
Disk IO Throughput, 151
Disk Usage, 151
Inodes, 152
Interface Traffic, 152
Load, 153
Memory Usage, 153
probes
nocpulse, 150
Process Count Total, 155
Process Counts by State, 154
Process Health, 155
Process Running, 156
Swap Usage, 156
TCP Connections by State, 157
Users, 158
Virtual Memory, 158
List Navigation
explanation of, 60
LogAgent
Log Pattern Match, 159
Log Size, 160
probes
nocpulse, 159

## M

macros
within configuration Files
interpolation, 108
Management
service level, 2
Monitoring, 115
All, 117
Critical, 117
Current State, 117
General Config, 118
introduction, 119
list of probes, 141
Notification, 118
OK, 117
Pending, 117
prerequisites, 119
Scout Config Push, 118
service level, 4
Status, 116
Unknown, 117
Warning, 117
MySQL
Database Accessibility, 161
Open Tables, 162
Opened Tables, 161
probes, 161
Query Rate, 162
Threads Running, 162

## N

navigation, 57
Network Services
  DNS Lookup, 163
  FTP, 163
  IMAP Mail, 164
  Mail Transfer (SMTP), 164
  Ping, 165
  POP Mail, 165
  probes, 163
  Remote Ping, 166
  RPCService, 167
  Secure Web Server (HTTPS), 167
  SSH, 168
  Web Server (HTTP), 168
notes
  about systems, 69
Notification
  filter, 118
notifications
  creating methods, 122
  deleting methods, 124
  filtering, 124
  Monitoring, 122
  receiving, 123
  redirecting, 123

## O

Oracle
  Active Sessions, 170
  Availability, 170
  Blocking Sessions, 170
  Buffer Cache, 171
  Client Connectivity, 171
  Data Dictionary Cache, 172
  Disk Sort Ratio, 173
  Idle Sessions, 173
  Index Extents, 173
  Library Cache, 174
  Locks, 175
  probes, 169
  Redo Log, 175
  Table Extents, 176
  Tablespace Usage, 176
  TNS Ping, 177
Organization Administrator, 114
overview of website, 57

## P

package installation
  scheduled, 4
package list
  Updating on server, 30, 70
packages
  details, 103
  downloading, 102
  filter, 100
  installing, 102
  overview, 102
password
  change, 62
preferences
  change, 63
probe
  guidelines, 141
probe list
  Apache
    Processes, 142
    Traffic, 142
    Uptime, 143
  General
    Remote Program, 147
    Remote Program with Data, 147
    SNMP Check, 148
    TCP Check, 149
    UDP Check, 149
    Uptime (SNMP), 150
  Linux
    CPU Usage, 150
    Disk IO Throughput, 151
    Disk Usage, 151
    Inodes, 152
    Interface Traffic, 152
    Load, 153
    Memory Usage, 153
    Process Count Total, 155
    Process Counts by State, 154
    Process Health, 155
    Process Running, 156
    Swap Usage, 156
    TCP Connections by State, 157
    Users, 158
    Virtual Memory, 158
  LogAgent
    Log Pattern Match, 159
    Log Size, 160
  MySQL
    Database Accessibility, 161
    Open Tables, 162
    Opened Tables, 161
    Query Rate, 162
    Threads Running, 162
  Network Services

DNS Lookup, 163
FTP, 163
IMAP Mail, 164
Mail Transfer (SMTP), 164
Ping, 165
POP Mail, 165
Remote Ping, 166
RPCService, 167
Secure Web Server (HTTPS), 167
SSH, 168
Web Server (HTTP), 168
Oracle
Active Sessions, 170
Availability, 170
Blocking Sessions, 170
Buffer Cache, 171
Client Connectivity, 171
Data Dictionary Cache, 172
Disk Sort Ratio, 173
Idle Sessions, 173
Index Extents, 173
Library Cache, 174
Locks, 175
Redo Log, 175
Table Extents, 176
Tablespace Usage, 176
TNS Ping, 177
RHN Satellite Server
Disk Space, 178
Execution Time, 178
Interface Traffic, 178
Latency, 179
Load, 179
Probe Count, 179
Process Counts, 180
Process Health, 181
Process Running, 182
Processes, 180
Swap, 182
Users, 182
WebLogic
Execute Queue, 144
Heap Free, 145
JDBC Connection Pool, 145
Server State, 146
Servlet, 146
probes
Apache, 142
General, 147
Linux, 150
LogAgent
nocpulse, 159
managing, 125
Monitoring, 125
MySQL, 161
Network Services, 163
on the RHN Server, 126
Oracle, 169
RHN Satellite Server, 177
thresholds, 125
WebLogic, 143
Provisioning
service level, 3
proxy server
with Red Hat Network Alert Notification Tool, 40
with Red Hat Network Registration Client, 44
with Red Hat Update Agent, 31


## Q


quality assurance
overview, 4
Quick Search
explanation of, 59


## R


reactivating
systems, 69
Red Hat Enterprise Linux 2.1
requiring the Red Hat Network Registration Client, i, 7
Red Hat Network
an introduction to, 1
components
primary, 1
Red Hat Network Alert Notification Tool
adding to panel, 39
applying Errata Updates, 41
configuring, 39
icons, 40
launching RHN website, 41
requirements, 39
with a proxy server, 40
Red Hat Network Configuration Client
rhncfg-client, 129
Red Hat Network Daemon, 37
configuring, 37
disabling, 37
initial description, 1
troubleshooting, 38
using to apply Errata Updates, 96
viewing status, 37
Red Hat Network Monitoring Daemon
(rhnmd) monitoring daemon, 119
installation, 120
probes requiring the daemon, 120
SSH key installation, 121
using sshd instead, 121
Red Hat Network Registration Client (rhn)_register)
initial description, 1

Red Hat Update Agent, 41
Command Line Arguments, 26
configuration, 30
with a proxy server, 31
Red Hat Update Agent (up2date)
activation keys, 34
choosing packages for update, 19
choosing software channels, 19
command line options, 26
command line version, 26, 33
configuration tool, 31
configuring general settings, 31
configuring package exceptions, 33
configuring retrieval and installation, 31
creating a user account, 11
excluding packages, 33
excluding packages from profile, 17
gathering RPM information, 15
graphical options, 8
initial description, 1
installing GPG keys, 28
installing packages, 24
log file, 30
registering a hardware profile, 14
registering a package profile, 15
registering a System Profile, 14
registering an organization account, 13
registering with, 9
setup and use, 18
starting, 7
synchronizing system profile, 30
reference guide
bug reporting, iv
conventions, i
introduction to the, i
registering
with activation keys, 34
Registration, 43
as part of an organization, 48
Configuration, 43
Email notification, 47
Hardware System Profile, 49
Password, 47
RPM Package List, 50
Software System Profile, 50
System Profile, 47, 49
text mode, 55
through the Web, 60
username, 47
with a proxy server, 44
with activation key, 85
RHN Satellite Server
Disk Space, 178
Execution Time, 178
Interface Traffic, 178
Latency, 179
Load, 179
Probe Count, 179
probes, 177
Process Counts, 180
Process Health, 181
Process Running, 182
Processes, 180
Swap, 182
Users, 182
RHN website, 41
initial description, 1
rhn-catalog
troubleshooting with, 126
rhn-runprobe
troubleshooting with, 127
rhnreg_ks, 85
rhnsd, 37
rhn_register
(See Registration)
RHUA; (up2date)
complete description, 7

## S

Schedule, 109
Scheduled Actions
Action Details, 111
Actions List, 110
Archived Actions, 110
Completed Actions, 110
Failed Actions, 110
Pending Actions, 110
Secure Sockets Layer, 5
security
overview, 4
service levels
Demo, 2
Management, 2
Monitoring, 4
Provisioning, 3
Update, 2
Software
Channel List
Channel Details, 99
Package Search, 101
searching, 101
software channels
details, 99
managers, 99
subscribers, 99
SSL expiration errors
connection
certificate verification, 5
subscribe to channel, 98
system group, 76

adding and removing, 78
creating, 78
deleting, 78
editing details, 78
list of, 76
viewing details, 78
system group list
status, 77
System Groups
assigning and removing, 73
joining and leaving, 73
System Group List, 76
system list, 66
System Profile, 49
Custom Information, 69
Notes, 69
Reactivation, 69
Updating hardware profile, 69
Updating package list, 30, 70
Updating Properties, 68
System Set Manager, 79
Systems
Advanced Search, 85
deleting, 68
Entitlements, 84
entitling, 84
overview, 65
searching, 85
System Details, 68
System List, 66
Systems Overview, 65
viewing a list of, 66
viewing details for, 68
systems list
status, 66
Systems Selected
explanation of, 59

## T

Troubleshooting
Monitoring, 126

## U

unsubscribe to channel, 98
Update
service level, 2
user account, 47
user details
modifying, 113
user roles, 114
users, 111
billing address, 115
changing email address, 114
changing password, 114
creating, 113
general address, 115
list of, 112
roles, 112, 114
shipping address, 115
User List, 112

## V

variables
macros
in configuration files, 108

## W

WebLogic
Execute Queue, 144
Heap Free, 145
JDBC Connection Pool, 145
probes, 143
Server State, 146
Servlet, 146
website, 57
activation keys, 85
All Errata, 96
Channel List, 97
Channels, 97
Config Channel List, 104
Configuration Channel Details, 106
Configuration File Details, 107
custom system information, 87
Errata, 94
Errata Search, 97
Help, 63
kickstart profiles, 87
logging in, 60
Monitoring, 115
navigation bar, 57
overview, 57
Purchase History, 63
Relevant Errata, 95
Schedule, 109
Software Channel Details, 99
Software Search, 101
stored profiles, 87
System Details, 68
System Entitlements, 84
System Group List, 76
System Groups, 76
System List, 66
System Search, 85
Systems, 65
Systems Overview, 65
Users, 111

Your Account, 62
Your RHN, 60

## Y

Your RHN, 60
Account Deactivation, 62
Addresses, 62
Email, 62
Help, 63
Purchase History, 63
Your Account, 62
Your Preferences, 63